Expt.-1

Date:

Introduction to AWS IAM

Aim: Learning about IAM role and usage of MFA

Theory: AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems in the cloud that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

the main purpose of the IAM is to enable a securely control access to AWS services and resources.With the help of AWS we can manage ,create policies to different users. they are many access authorizes to users like giving access keys , passwords and multi-factor authentication devices.

we can create roles and add permissions to control which operation can be performed by the entity.

In this post i will show you

- pre-created users are added to the groups
- Updating Passwords for the users
- How we can edit a group policy
- Locating and using the IAM sign-in URL

Working:

List of instructions in creating a IAM in Amazon Web Services

Step 1- Exploring the Users and Groups

1. Log in into AWS console with your user credentials

2. Click on **Services**
3. Now click on **IAM** or **Identity Access Management**
4. you can able to view a dashboard and some list of options in the left navigation pane.Click on **Users** and **Groups** to see the list of 3 users and 3 groups. NOTE: these are pre-created users and groups that I have in this lab

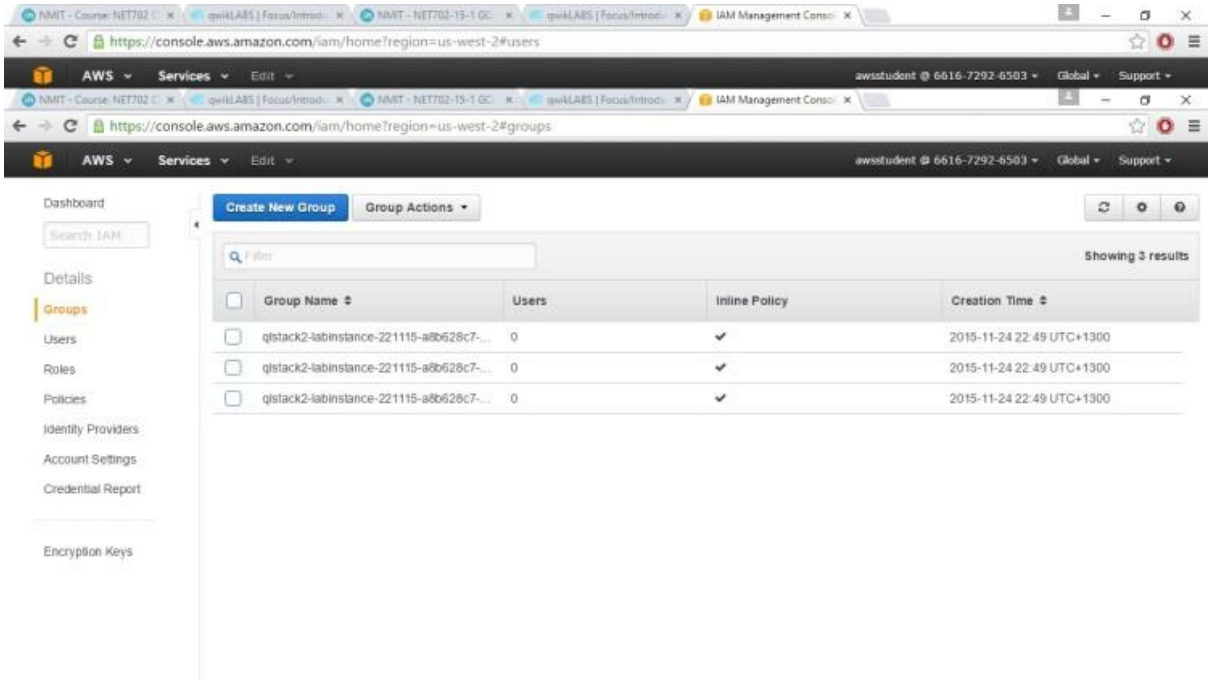


Figure 1.1 Creating new group

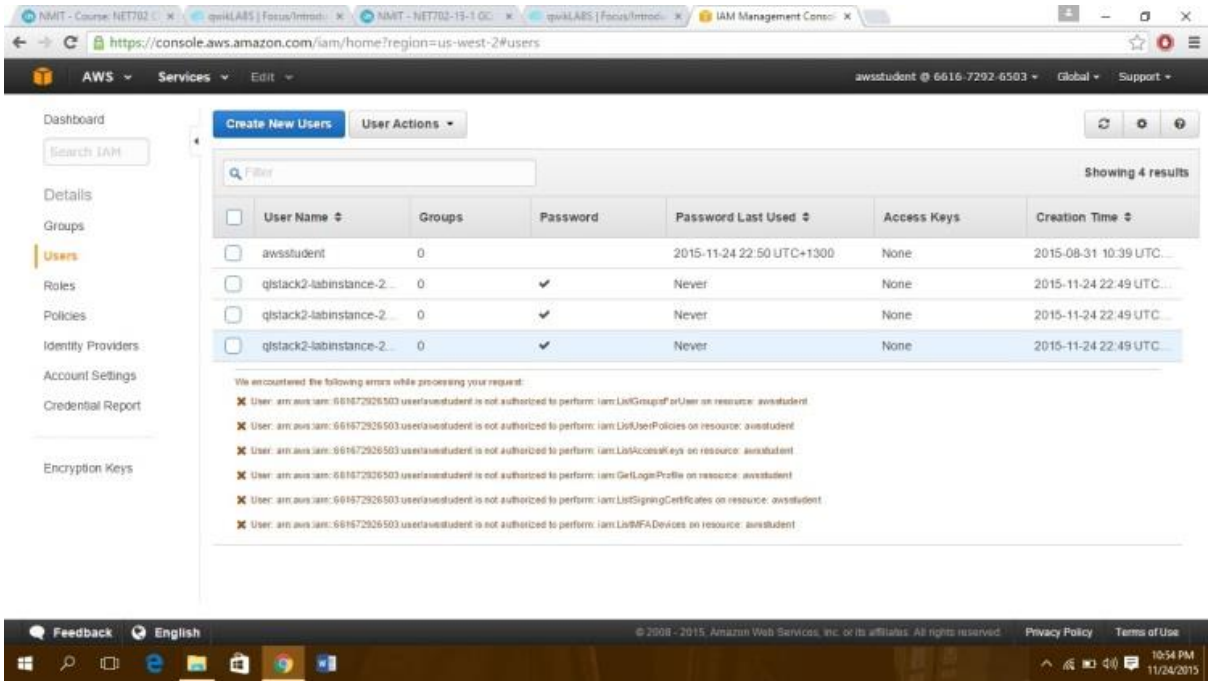


Figure 1.2 Creating new users

THE USERS LIST IS

- **qlstack2-labinstance-221115-a8b628c7-0192-usertwo-1TRQWGCV75Z2**
- **qlstack2-labinstance-221115-a8b628c7-019-userthree-J928R1RQVS04**
- **qlstack2-labinstance-221115-a8b628c7-0192-userone-55B3I6FWOJVM**

Find the userone and and click on its name to get the details 0f the user. it shows the following properties

- Permissions given to the user
- groups associated with the user
- security credentials

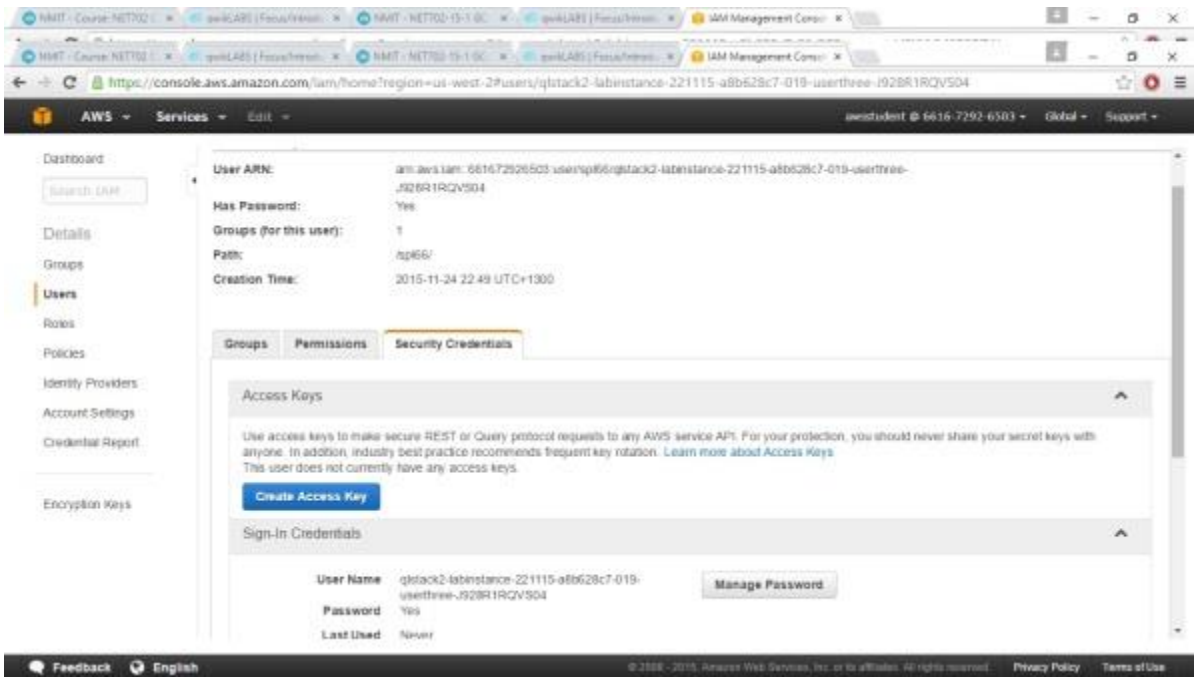


Figure 1.3 click on manage password and generate a new password as below

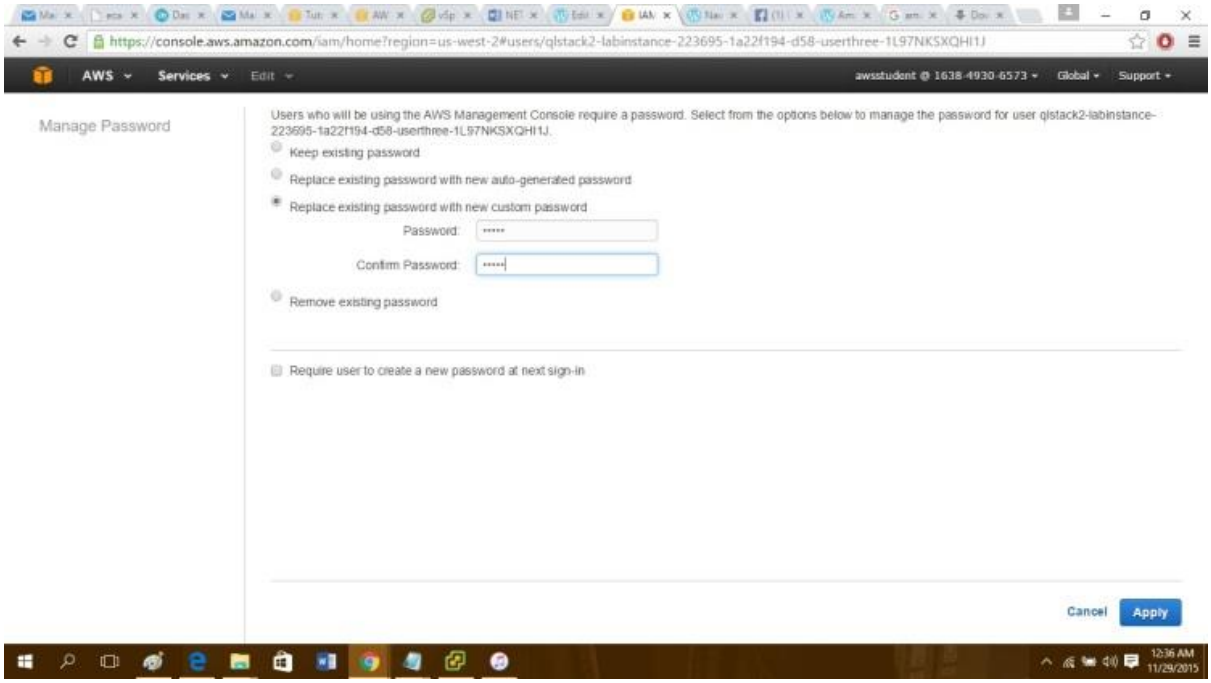


Figure 1.4 The password has been successfully changed, but it has been not associated to any groups and policies.

THE GROUP LIST IS

- **qlstack2-labinstance-223695-1a22f194-d5-EC2support-6LS7EKDQIGIX**
- **qlstack2-labinstance-223695-1a22f194-d584-EC2admin-127HSQ3N2AOM8**
- **qlstack2-labinstance-223695-1a22f194-d584-S3admin-1FSDTQK9NBKDZ**

its a big and huge names we make these simple by noting them as

- user-one
- user-two
- user-three

and group's name as

- EC2support
- EC2admin
- S3admin

click on each name to get the properties where you can see the users assigned to the group and permissions given to the group

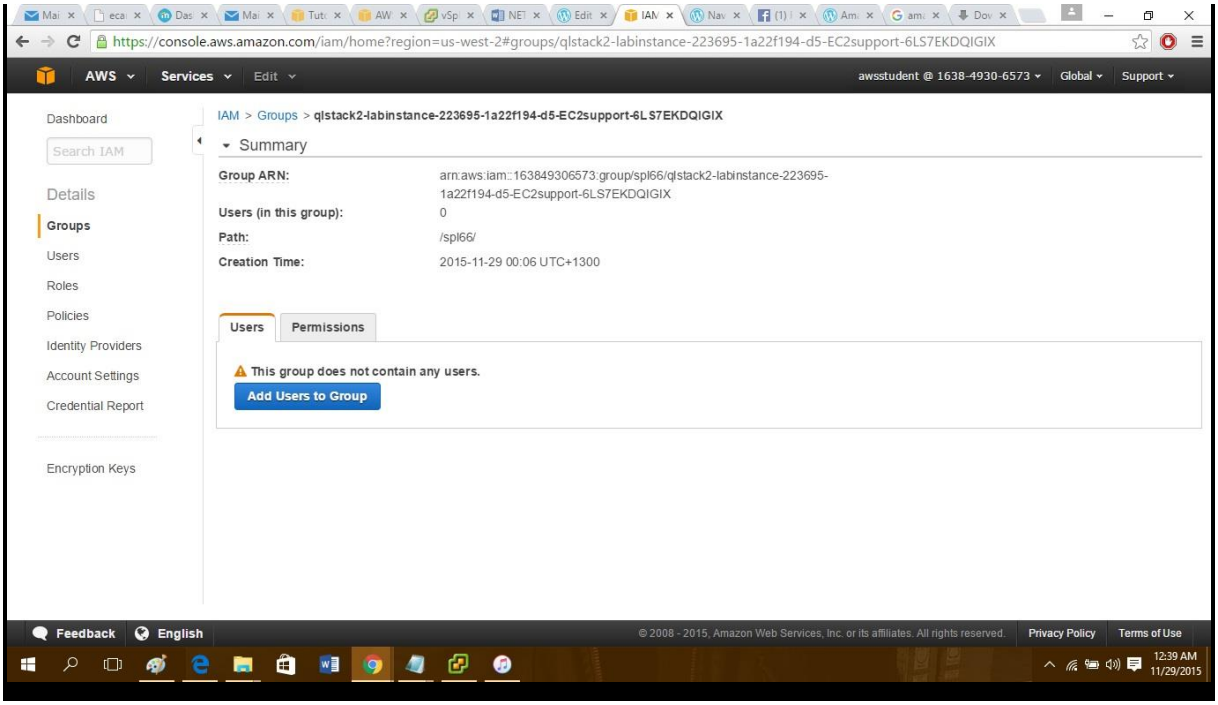


Figure 1.5 Adding users to the group

Step2 -Adding Users to Groups

Accessing or giving permissions to the user with a group policy. Lets take **userone** user and add it to the **EC2support** group . Where they will be attached with a **EC2supportpolicy.**

- goto **services** and click **IAM .** In the left pannel , click **groups.** Click on the "**EC2support"** group
- Under the users section and click **Users to the group**
- Select "**userone"** and click the blue "**Add Users"** button in the lower right
- When you finish , you can check the groups list where the EC2Support group have a "1" in the user column.
- follow these steps and assign the two groups to two users.

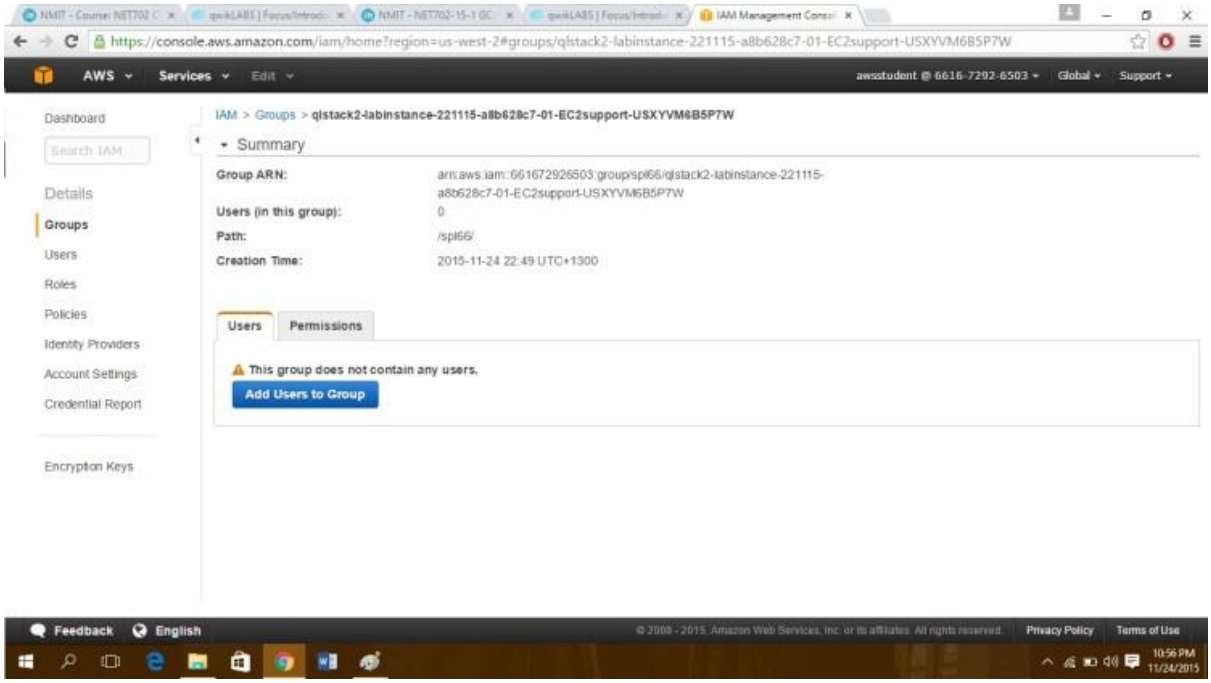


Figure 1.6 click on add users to group to add user and associate a group policy

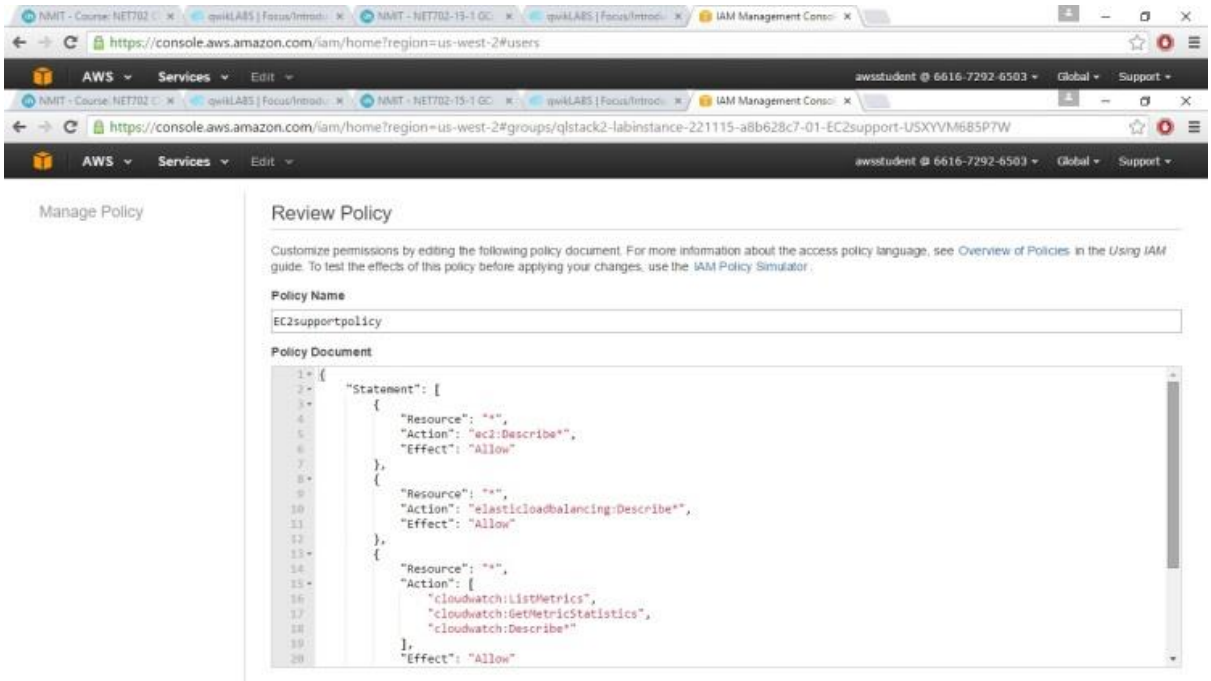


Figure 1.7 editing the policy associated to the user

Step 3 -Testing the Access

we had successfully assigned the users to the each group. After the assigning try to test the user at storage service s3 console application.

1. goto **IAM** and **USERS** click on **userone**

2. click on **security credentials** you can able to see the username just **COPY** the username and paste in temporary notepad file
3. **signout** from the aws user and login with the **userone** username and updated password.
4. click on **services** and **s3**

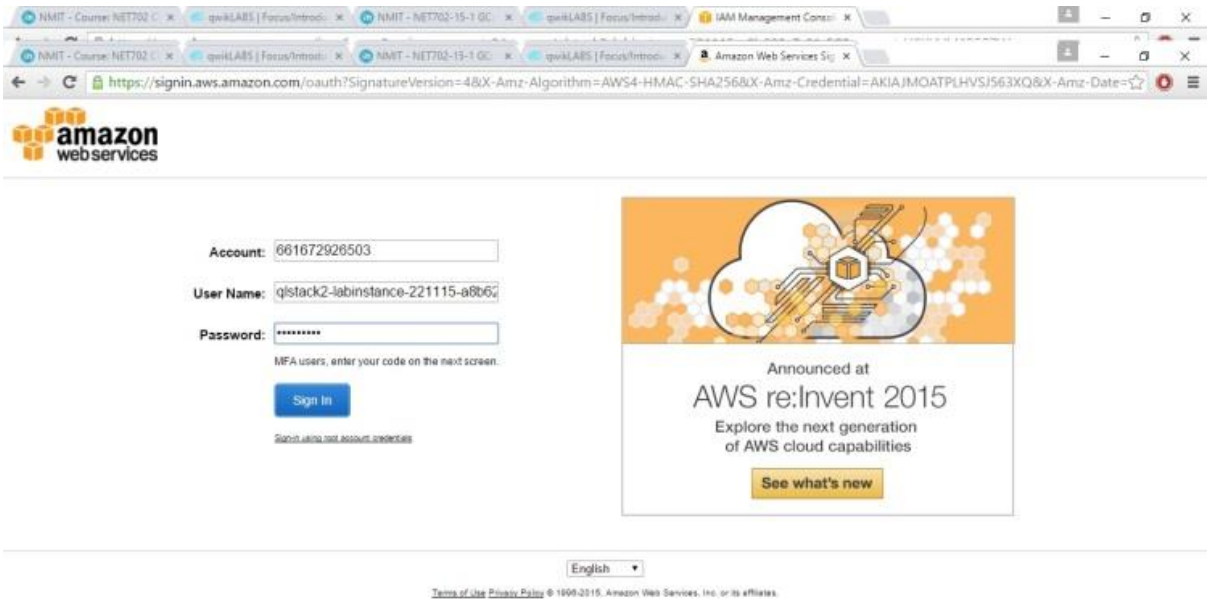


Figure 1.8 log in into the aws account with your new user credentials

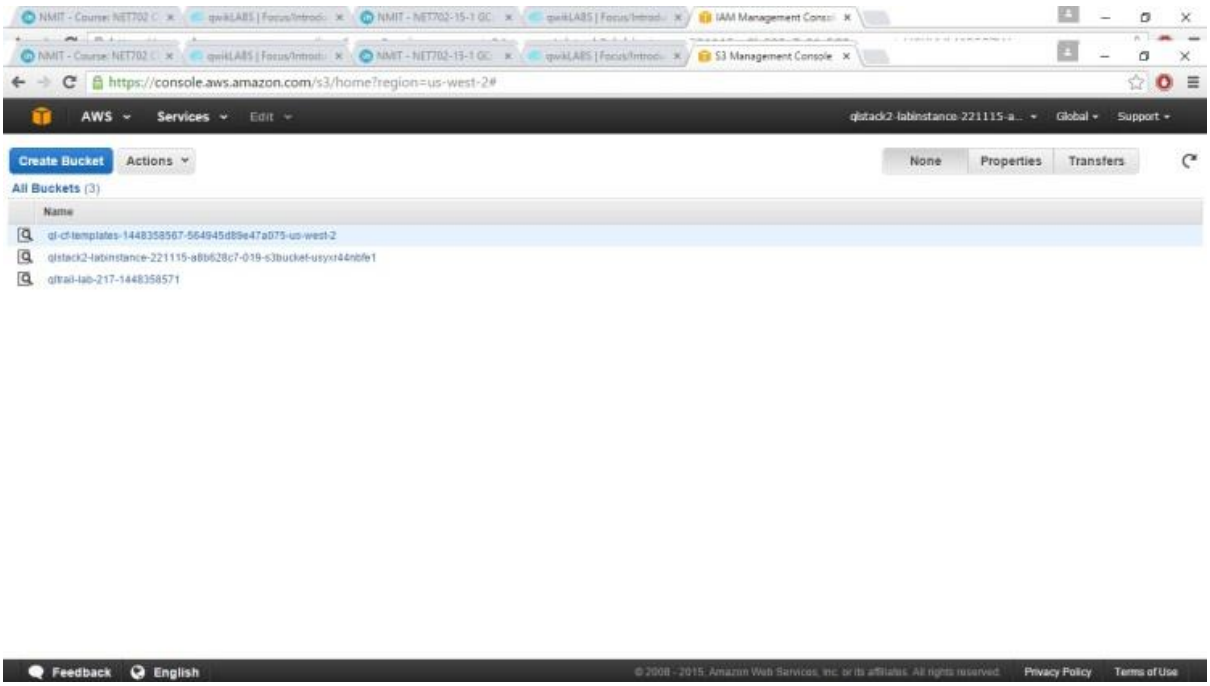


Figure 1.9 user can able to see and mange the storage accounts in S3

5. follow the same login process using usertwo credentials and check the access of the user.

By clicking on **services** and **s3**

This user don’t have permissions to view the storage files.

if you follow the steps you will get the following message

Figure 1.10

Finally we learned

- Explored pre-created IAM users and groups
- Inspected IAM policies as applied to pre-created groups
- adding users to group and managing the passwords
- review the policy and managing the group policy

Result: The experiment was successfully executed on AWS Console in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-2

Date:

Aim: Launching and connecting EC2 of windows and Linux

Theory: Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

The instance launched is an Amazon EBS-backed instance (meaning that the root volume is an EBS volume). You can either specify the Availability Zone in which your instance runs, or let Amazon EC2 select an Availability Zone for you. Availability Zones are multiple, isolated locations within each Region. You can think of an Availability Zone as an isolated data center. When you launch your instance, you secure it by specifying a key pair (to prove your identity) and a security group (which acts as a virtual firewall to control ingoing and outgoing traffic). When you connect to your instance, you must provide the private key of the key pair that you specified when you launched your instance.

Working: To launch an instance

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the EC2 console dashboard, in the **Launch instance** box, choose **Launch instance**, and then choose **Launch instance** from the options that appear.
3. Under **Name and tags**, for **Name**, enter a descriptive name for your instance.

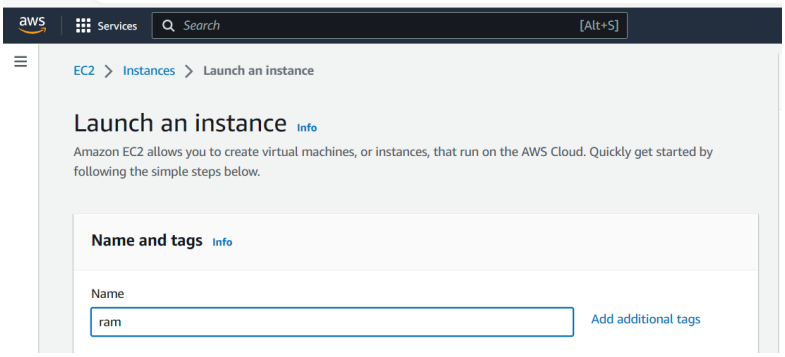


Figure 21.Enter a descriptive name for the instance

4. Under **Application and OS Images (Amazon Machine Image)**, do the following:
    a. Choose **Quick Start**, and then choose Amazon Linux. This is the operating system (OS) for your instance.
    b. From **Amazon Machine Image (AMI)**, select an HVM version of Amazon Linux 2. Notice that these AMIs are marked **Free tier eligible**. An *Amazon*

Machine Image (AMI) is a basic configuration that serves as a template for your instance.

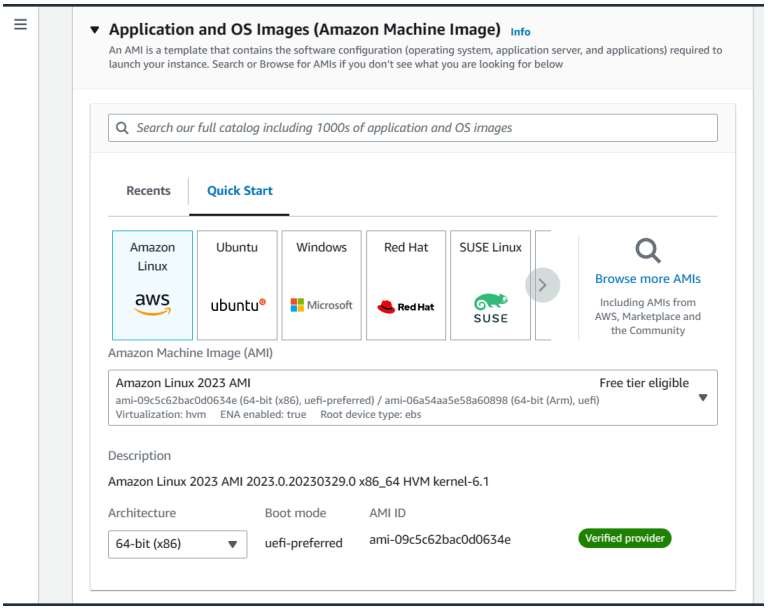


Figure 2.2 Machine Image

5. Under **Instance type**, from the **Instance type** list, you can select the hardware configuration for your instance. Choose the t2.micro instance type, which is selected by default. The t2.micro instance type is eligible for the free tier. In Regions where t2.micro is unavailable, you can use a t3.micro instance under the free tier. For more information, see [AWS Free Tier].

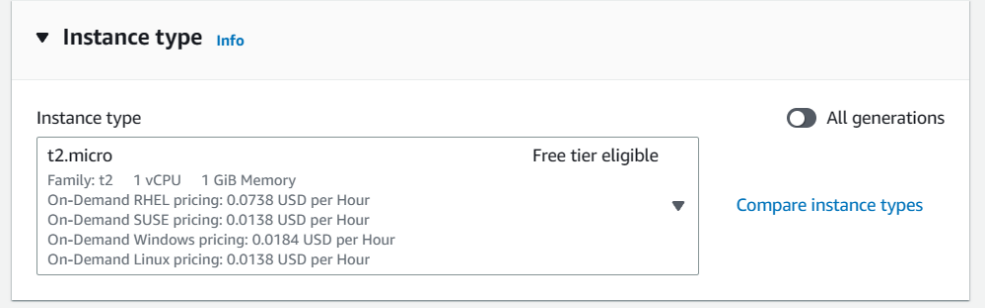


Figure 2.3 Select Instance type

6. Under **Key pair (login)**, for **Key pair name**, choose the key pair that you created when getting set up.

Warning

Do not choose **Proceed without a key pair (Not recommended)**. If you launch your instance without a key pair, then you can't connect to it.

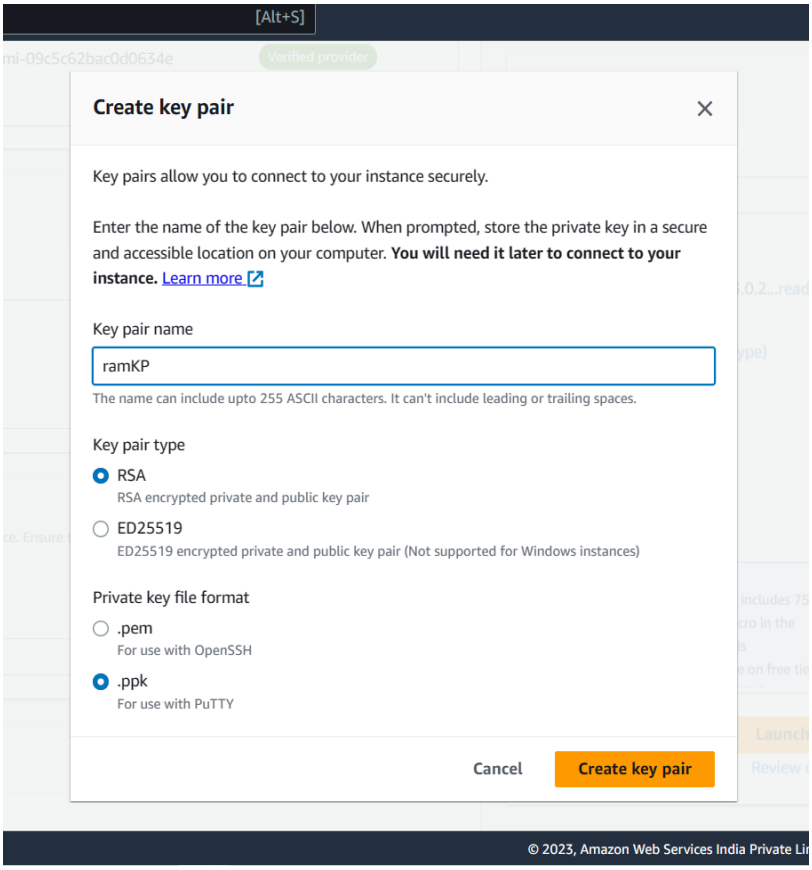


Figure 2.4 Create key pair

7. Next to **Network settings**, choose **Edit**. For **Security group name**, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
    a. Choose **Select existing security group**.
    b. From **Common security groups**, choose your security group from the list of existing security groups.

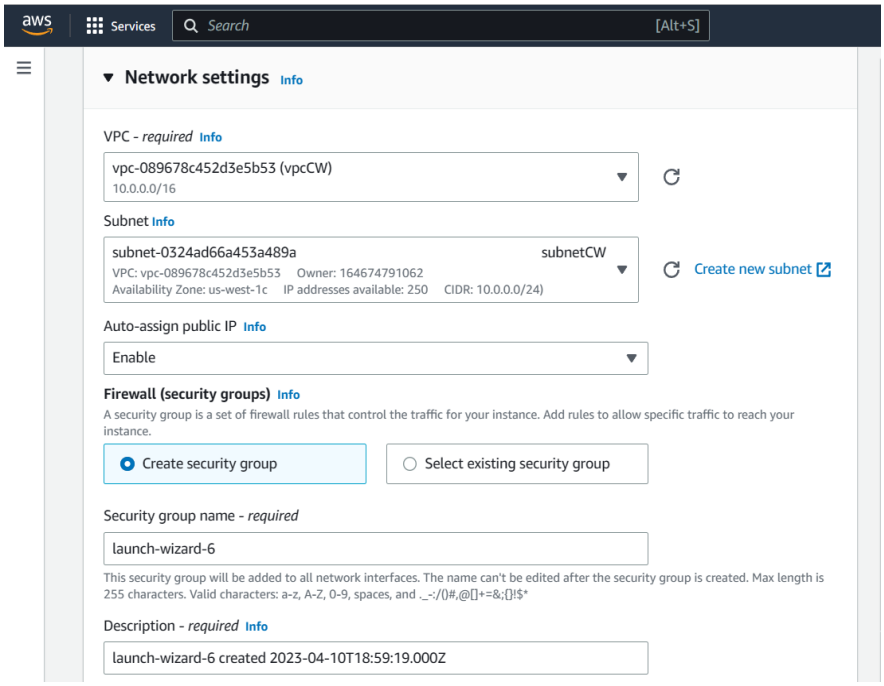


Figure 2.5 Choose security group

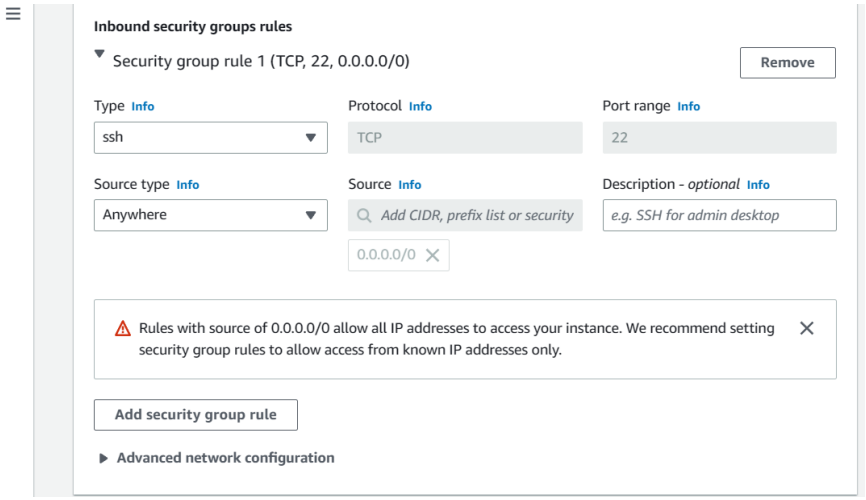


Figure 2.6

8. Keep the default selections for the other configuration settings for your instance.

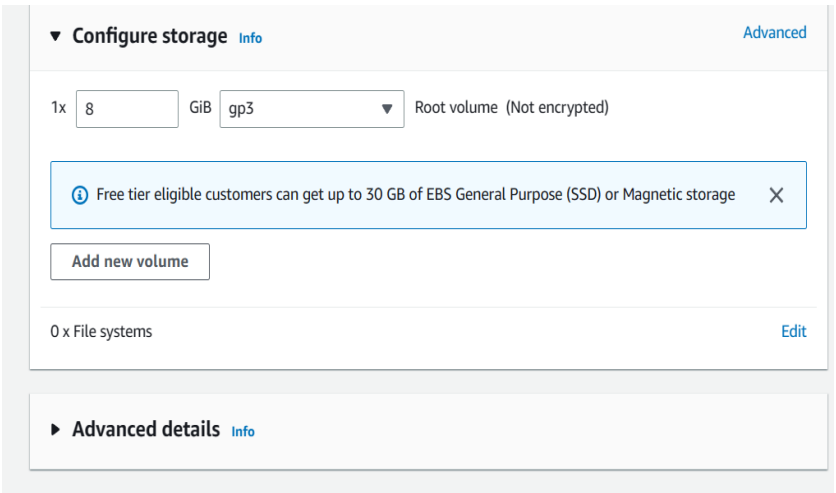


Figure 2.7 Keep default selections for other configurations

9. Review a summary of your instance configuration in the **Summary** panel, and when you're ready, choose **Launch instance**.

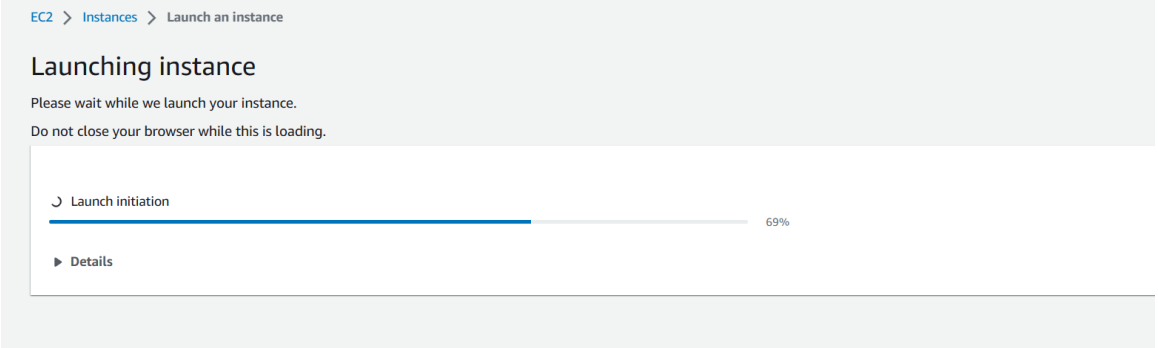


Figure 2.8 Launching Instance

10. A confirmation page lets you know that your instance is launching. Choose **View all instances** to close the confirmation page and return to the console.

Figure 2.9 Confirmation page

11. On the **Instances** screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name. If the **Public IPv4 DNS** column is hidden, choose the settings icon (⚙) in the top-right corner, toggle on **Public IPv4 DNS**, and choose **Confirm**.
12. It can take a few minutes for the instance to be ready for you to connect to it. Check that your instance has passed its status checks; you can view this information in the **Status check** column.

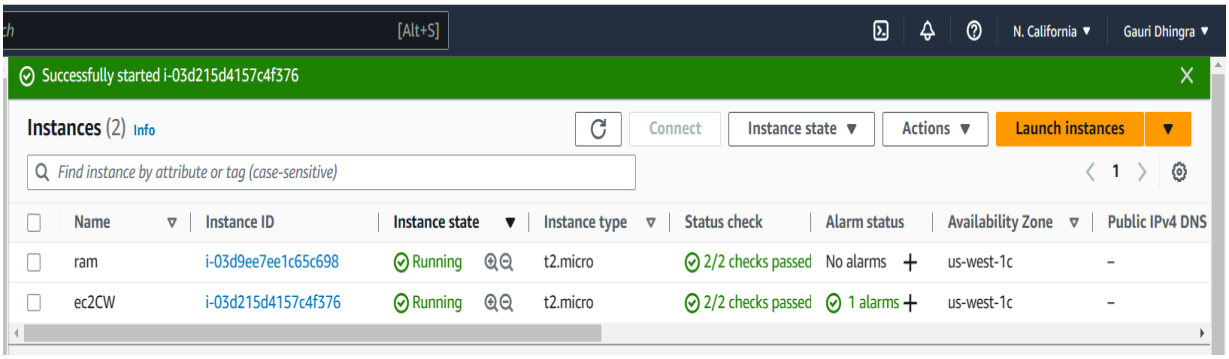


Figure 2.10

To conncet to PuTTY follow the steps below:

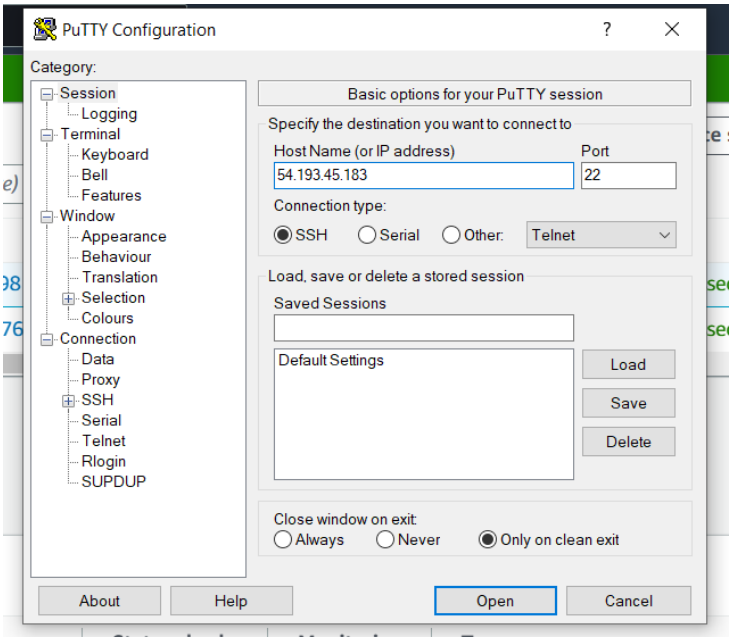


Figure 2.11 Select ssh then auth:

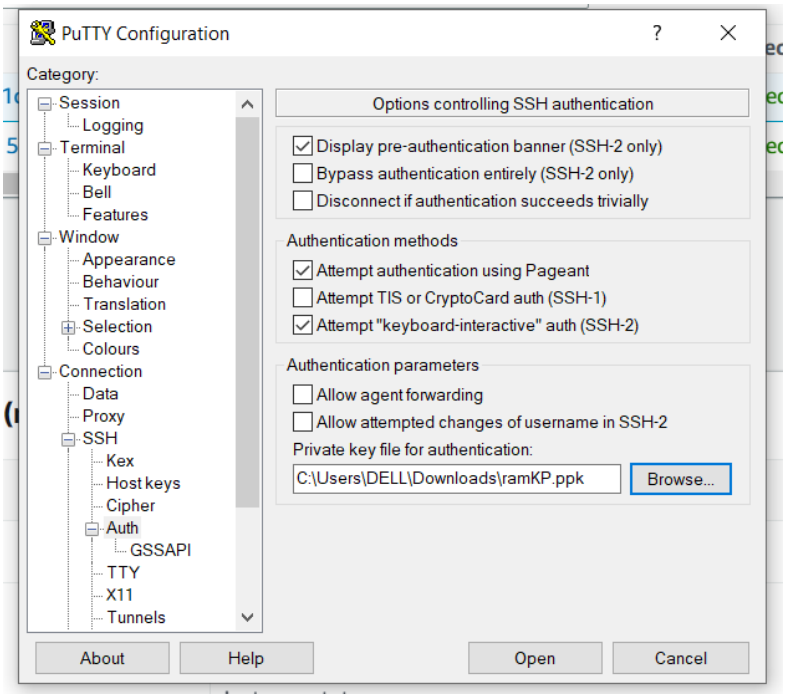


Figure 2.12

Figure 2.13 login as ec2-user

Result: The experiment was successfully executed on AWS Console in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-3

Date:

Aim: Amazon Lambda

Let's start by creating a Lambda Function.

- After setting the AWS Account.
- Go and type **AWS Lambda** in your AWS Management console.
- Click on Create a Function.

You'll see a setup page shows up where you have to fill up few aspects for your function

as the name, runtime, role, you can choose from blueprints as well but here we're going to author it from scratch.

- Enter the name and all the credentials, now in case of the runtime, you can choose any based on your understanding of that language, we're choosing NodeJS 8.10, here you can choose from any option like python, java, .Net, Go (these are the languages it supports).
- Then create a role, you'll have to create a new role if you don't have one, either you create a new template for the role or leave the template blank.
- Like in our case, we've chosen an existing role that we have created
- As here we have already defined our role with the name of *service-role/shubh-intel*.
- The next step after this is **Writing Code** for your Lambda Function.
- We're choosing **Lambda Console** here, you can choose from different code editors like

  Cloud9 Editor or on your Local machine.

- You can check your function being created, as here we have created it with the name

  of *example-lambda*.

When you created the function, you will be directed to a **Function Code** screen, where

you will be defining your function, either you can choose the code from below or you can make your own template for it, it's quite easy.

exports. Handler = async (event) => {// TODO implement return 'Hello from Lambda!' };

• If you want to define the key value then you can, like here we've defined key1 and key2

and key 1= 'Hello from Lambda!'

- Then create the event like we created it with the name of *mytestevent* click **Save and**

  Test in order to run your function.

- After running it, you will get an output where you check the details and you will get the output as below:

Screenshots:

Figure 3.1

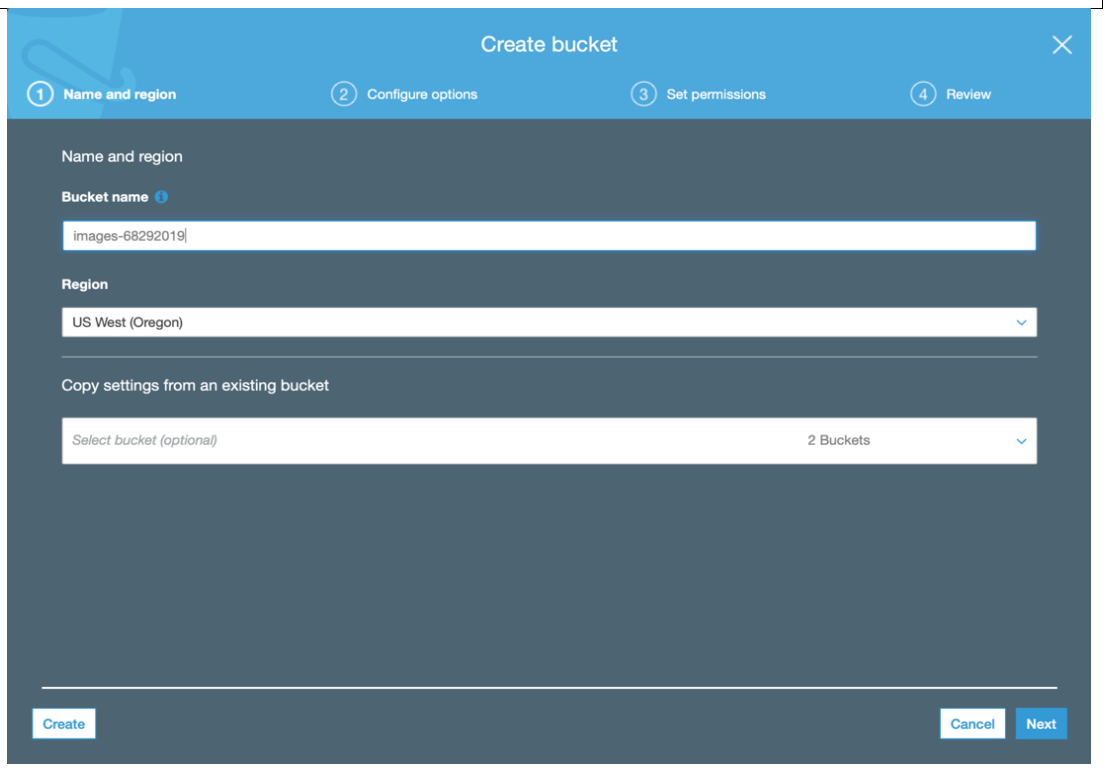


Figure 3.2

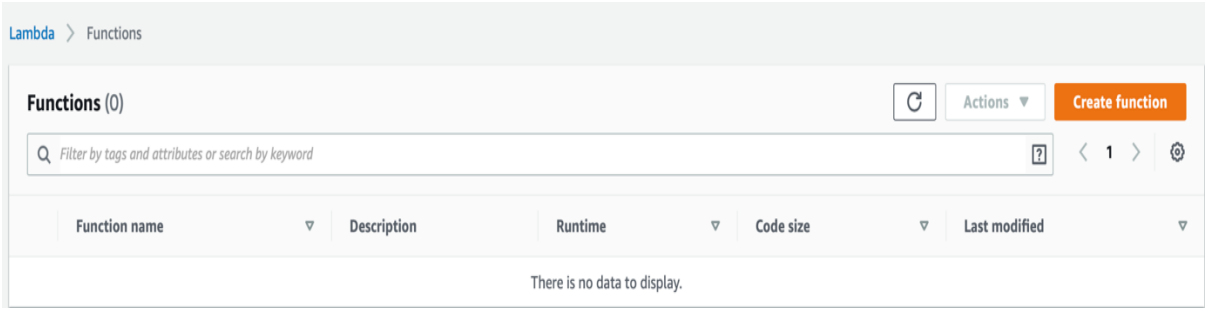


Figure 3.3

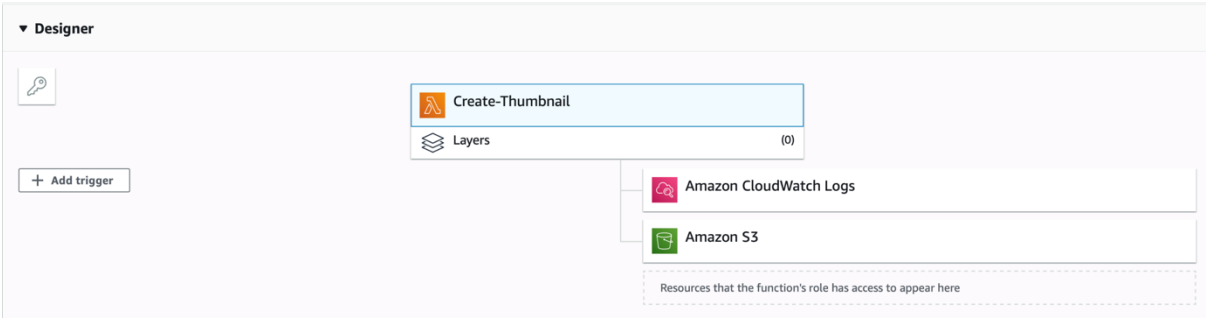


Figure 3.4

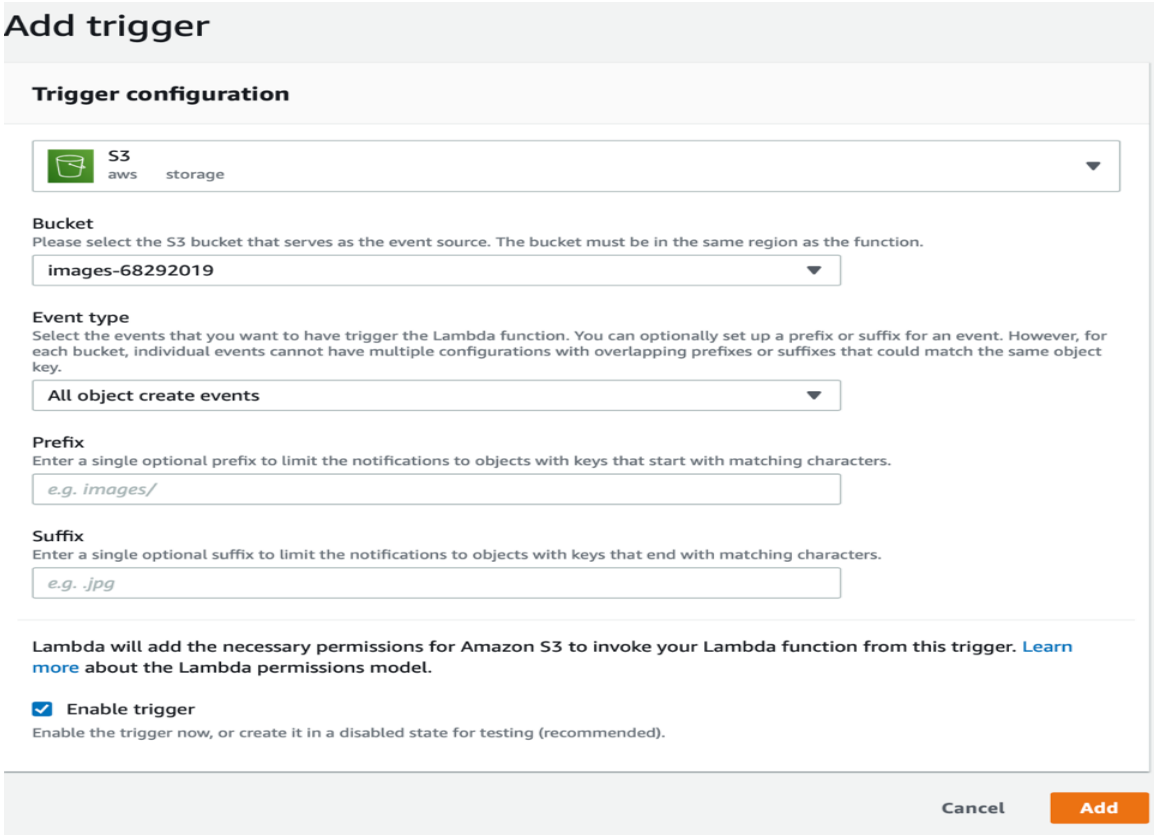


Figure 3.5

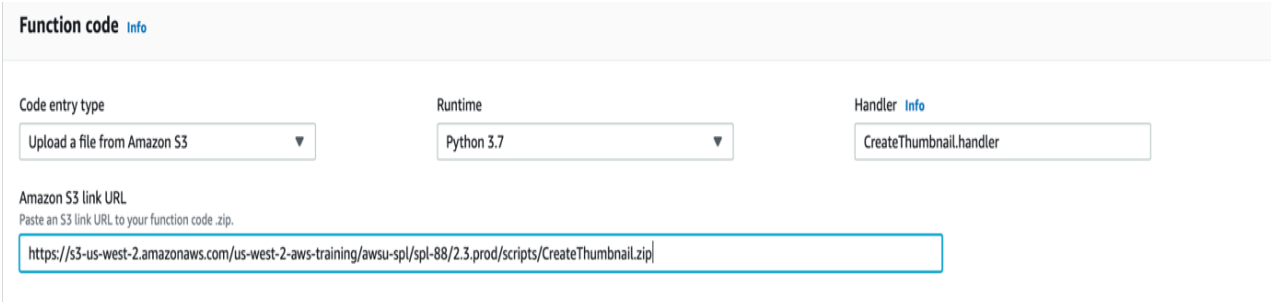


Figure 3.6

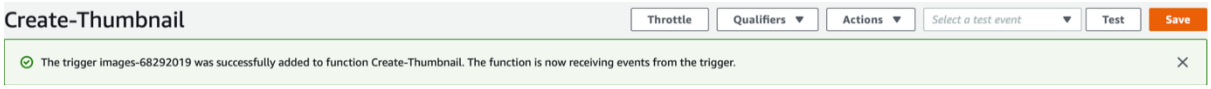


Figure 3.7

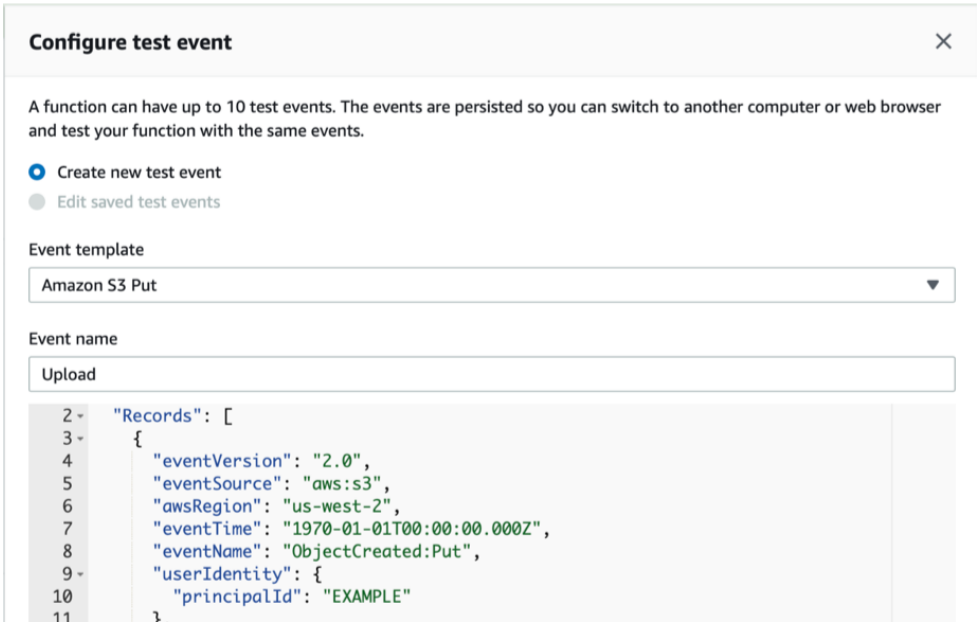


Figure 3.8

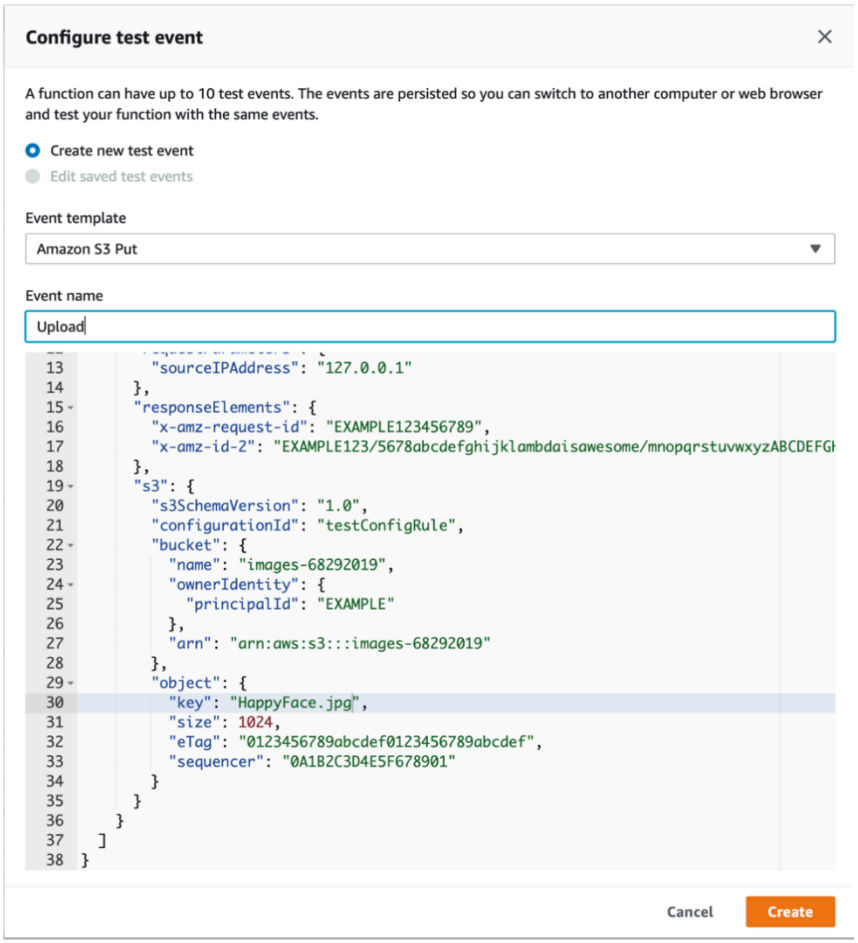


Figure 3.9

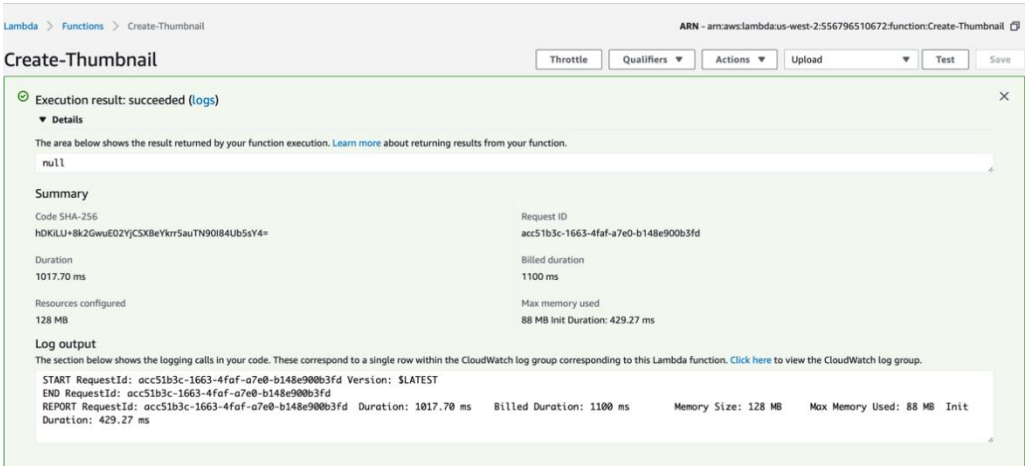


Figure 3.10

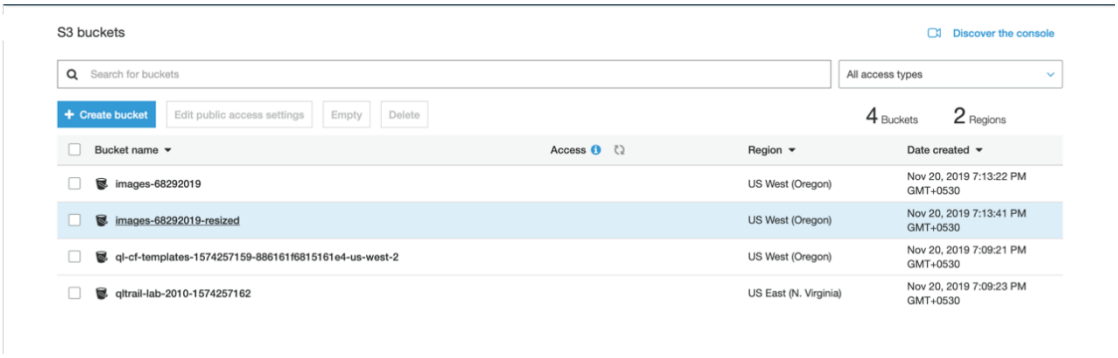


Figure 3.11

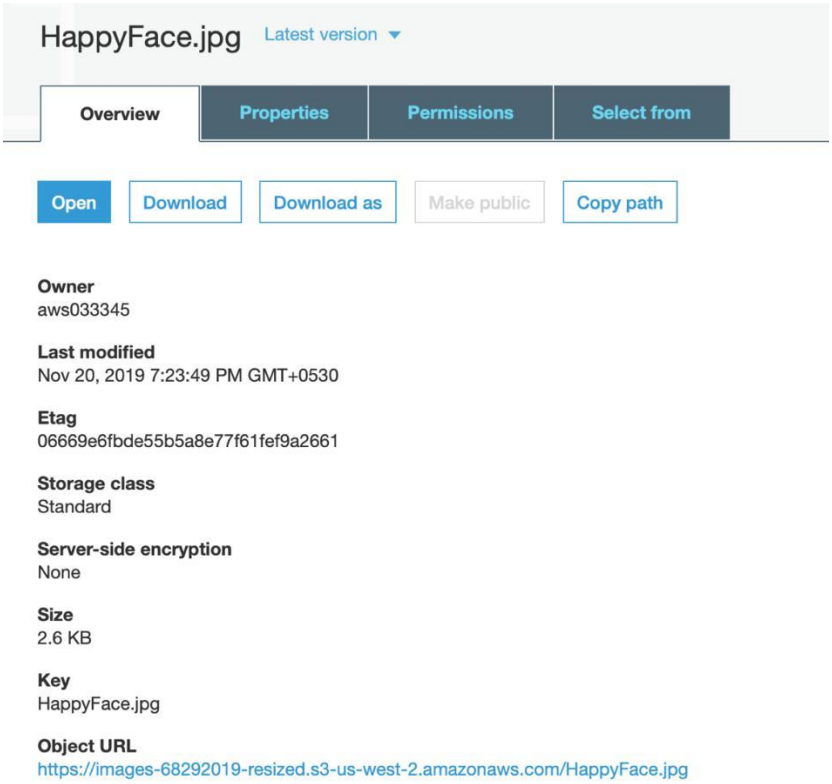


Figure 3.12

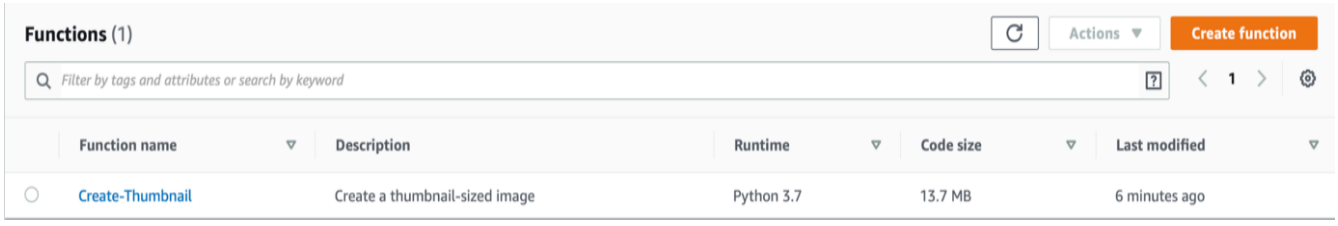


Figure 3.13

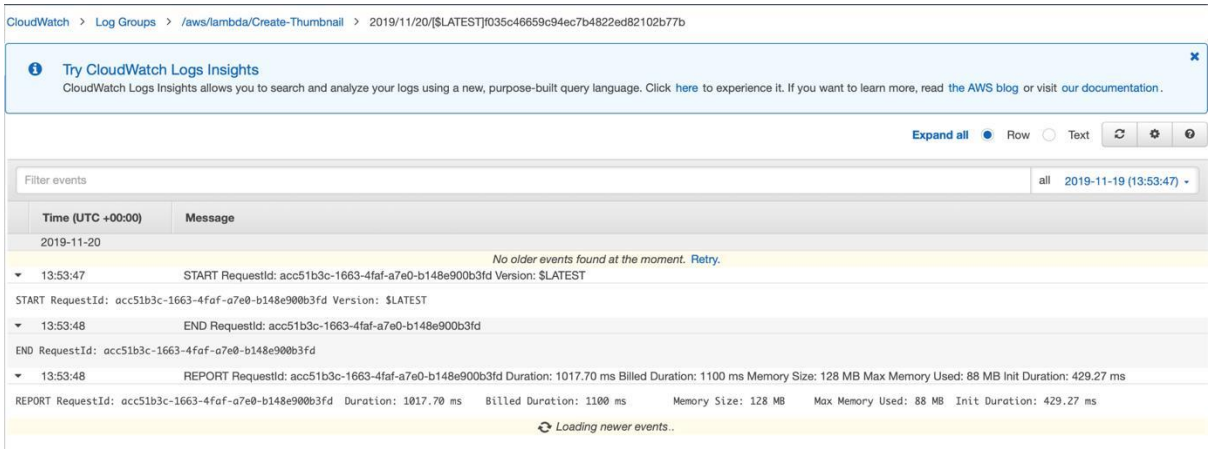


Figure 3.14

Figure 3.15

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-4

Date:

Aim: Working with EBS

Theory: Amazon Elastic Block Store (EBS) is providing persistent high performance block storage service at any scale and designed for use with EC2 instances. EBS facilitates to deployed huge workload such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems and EBS volumes are highly available, also highly reliable volumes. because Amazon EBS volumes are automatically replicated on the backend. EBS have ability to create point-in-time consistent snapshots of the volumes.

Working:

Task 1: Create a New EBS Volume

Open the **AWS Management Console** –> click **Services** menu –> click **EC2** –> click **Instances** –> Note the **Availability Zone** of the instance (us-east-1a) –>

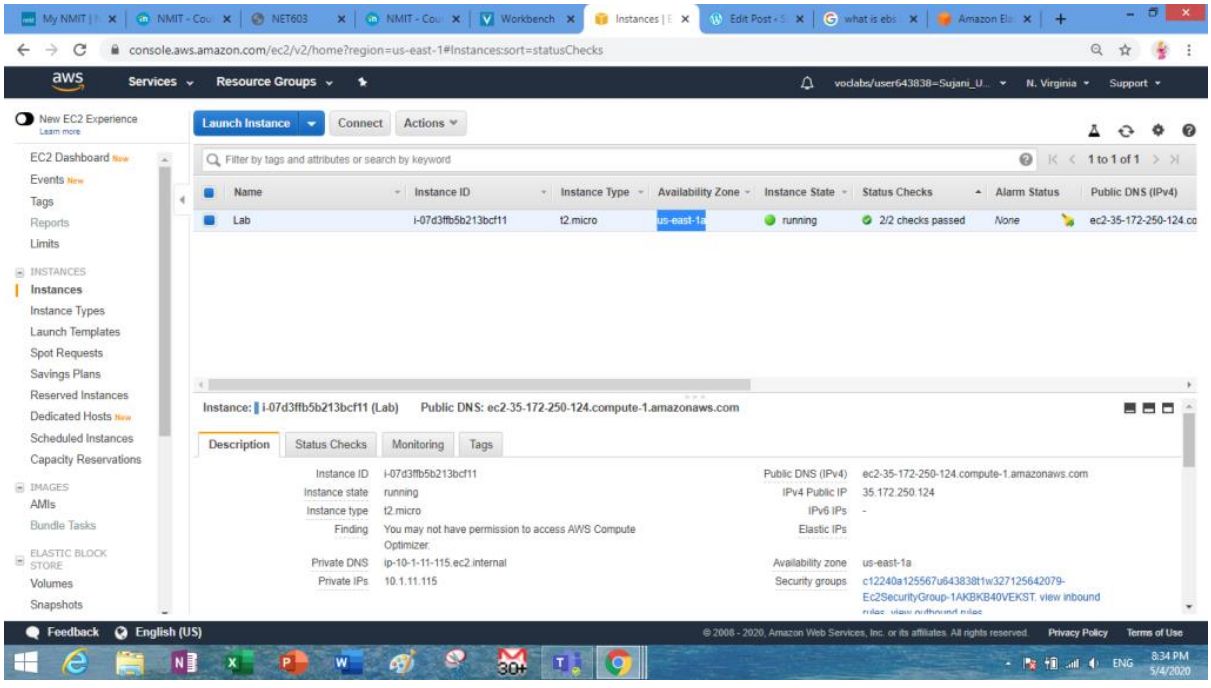


Figure 4.1

click **Volumes** (we can see a 8 GiB volume attached to the Lab instance) –> Click **Create Volume** –>

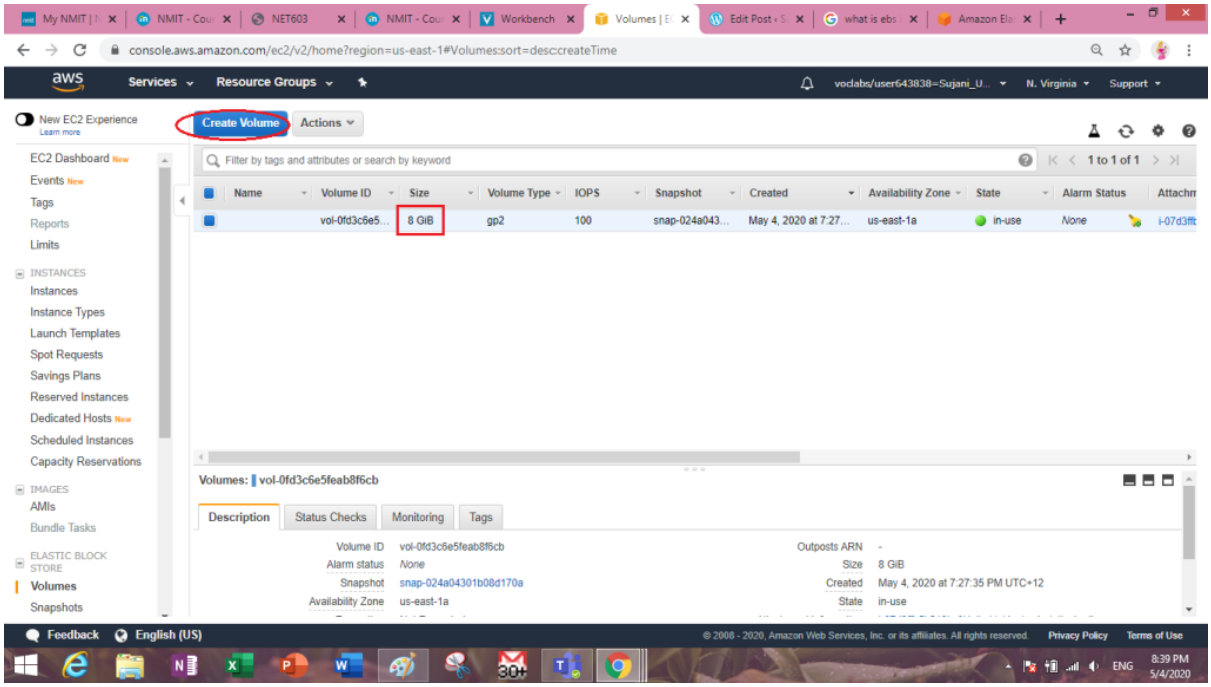


Figure 4.2 Create volume

Apply following configurations:

- **Volume Type:** *General Purpose SSD (gp2)*
- **Size (GiB):** 1
- **Availability Zone:** us-east-1

Click **Add Tag** –> add following text in Tag Editor:

- **Key:** Name
- **Value:** My Volume

Click **Create Volume** button –>

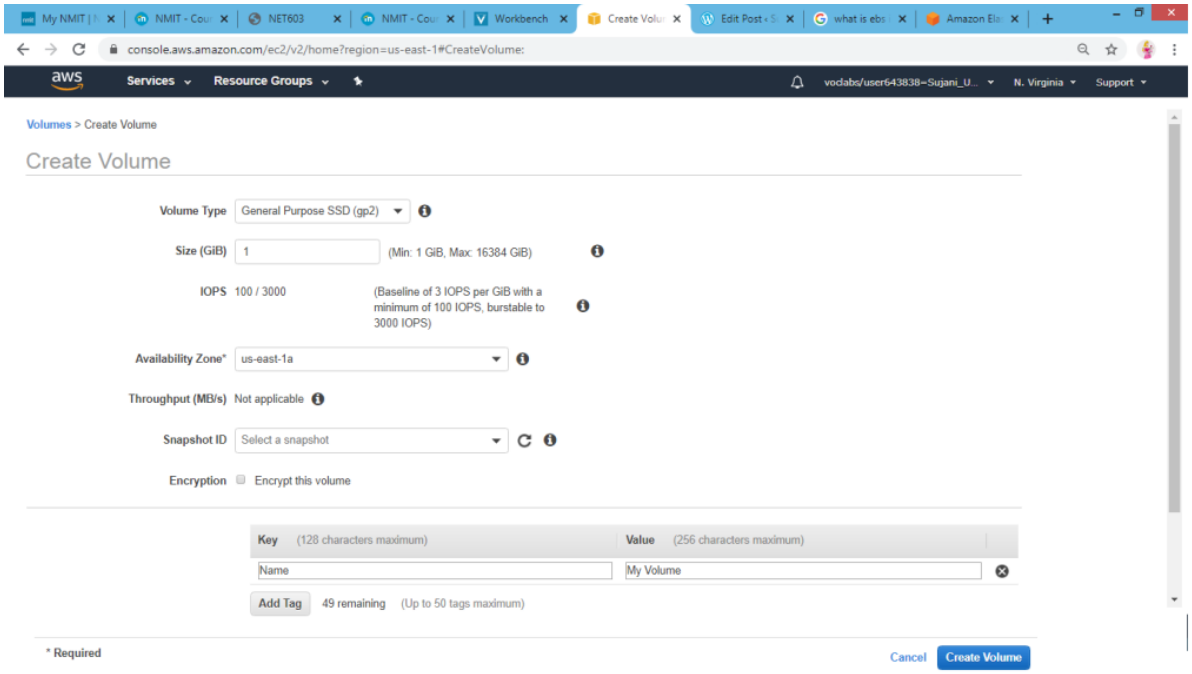


Figure 4.3

click **Close** –>

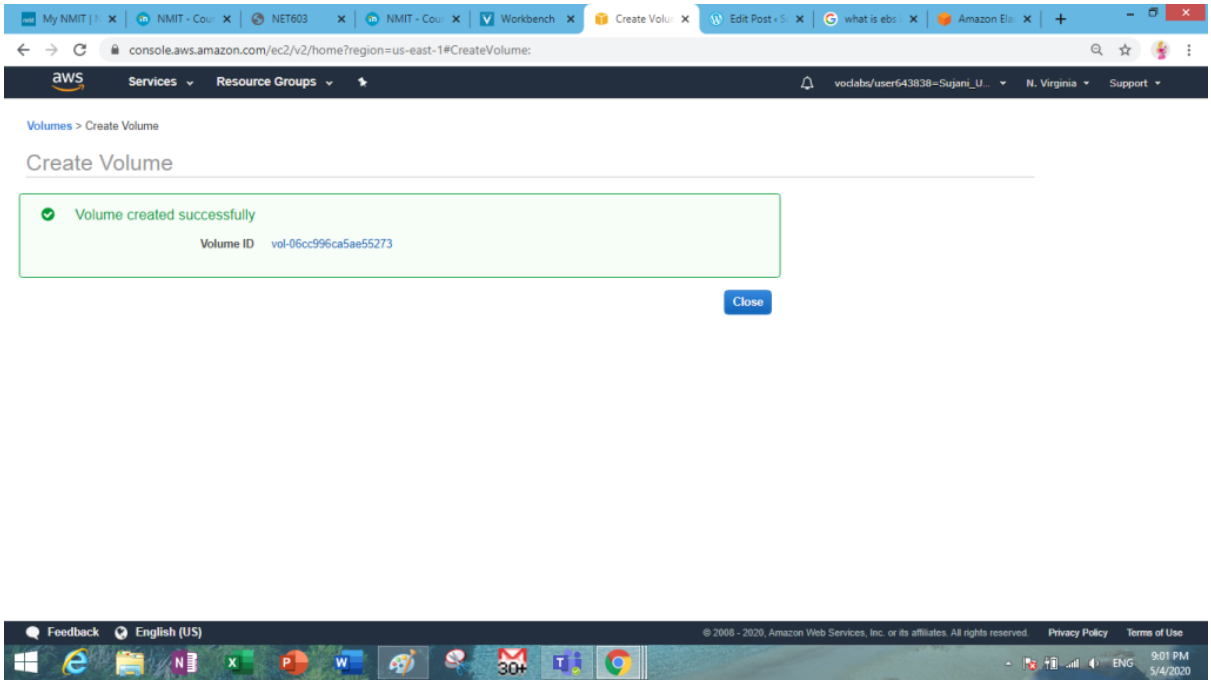


Figure 4.4 Volume created

we can see the new volume ID= vol-06cc996ca5ae55273 with 1GiB

Note: state of new volume is available (still not in-use)

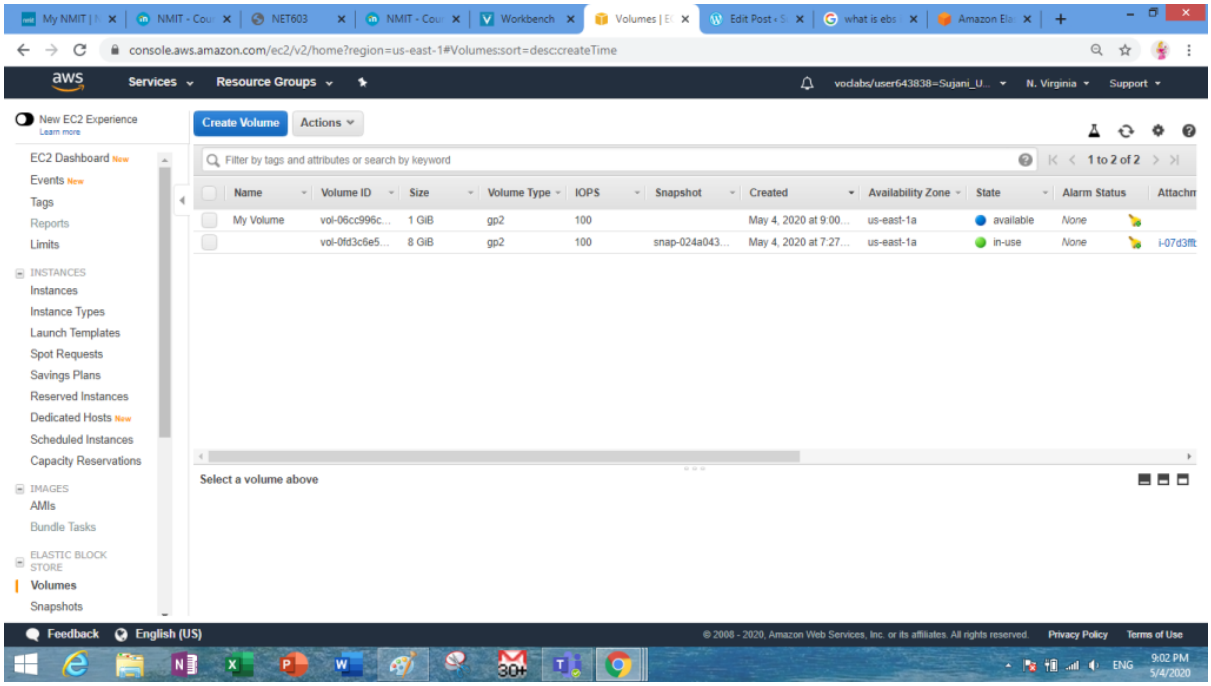


Figure 4.5

Task 2: Attach the Volume to an Instance

Select **My Volume** –> click **Attach Volume** in the **Actions** menu –>

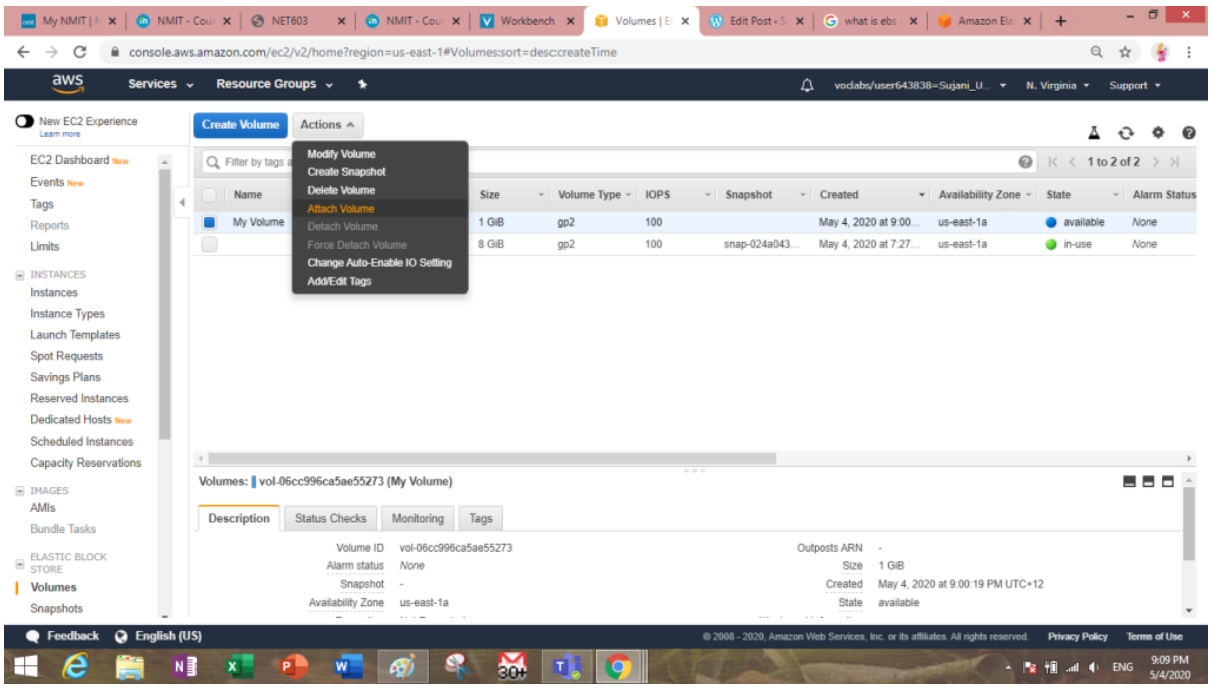


Figure 4.6

Click in the **Instance** field –> select the instance (Lab) –> Device field is automatically selected **/dev/sdf** –> Click **Attach** –>

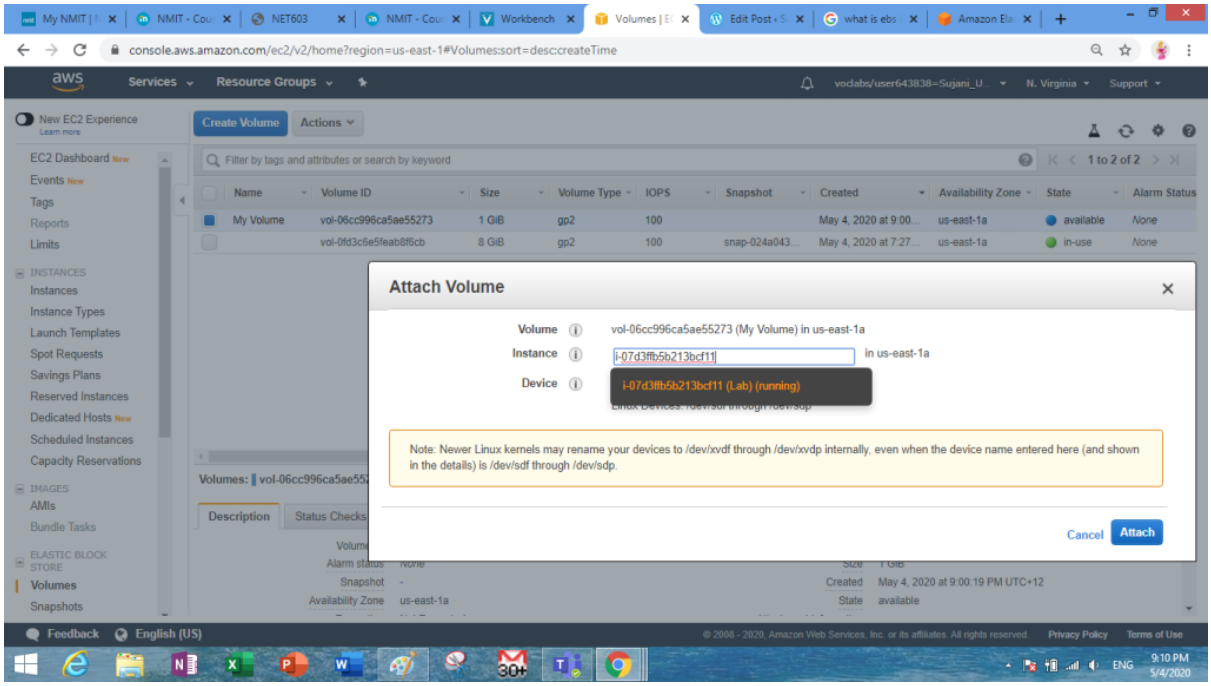


Figure 4.7

Note: Instance state now change into **in-use**

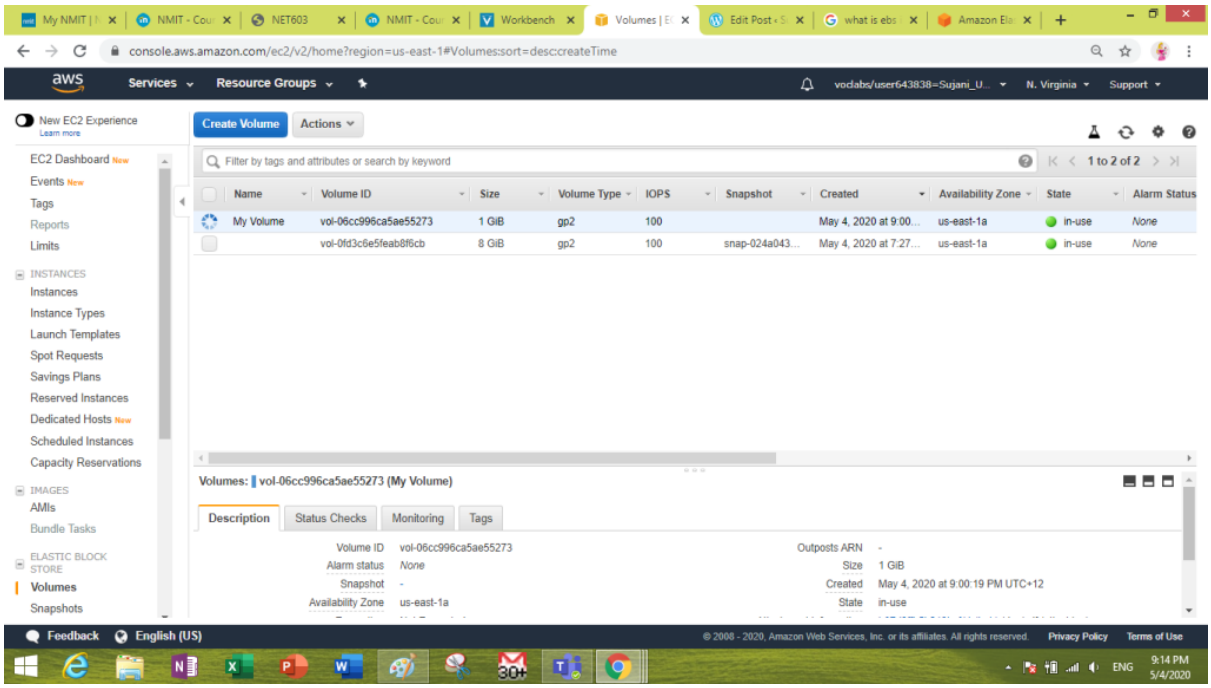


Figure 4.8 Instance state change into in-use

Task 3: Connect to Your Amazon EC2 Instance

First we have to make the SSH connection from our PC.

I am using a windows PC and following configurations are only for the windows SSH connection.

Click on the **Details** button in the instruction page –> click **Show** –>

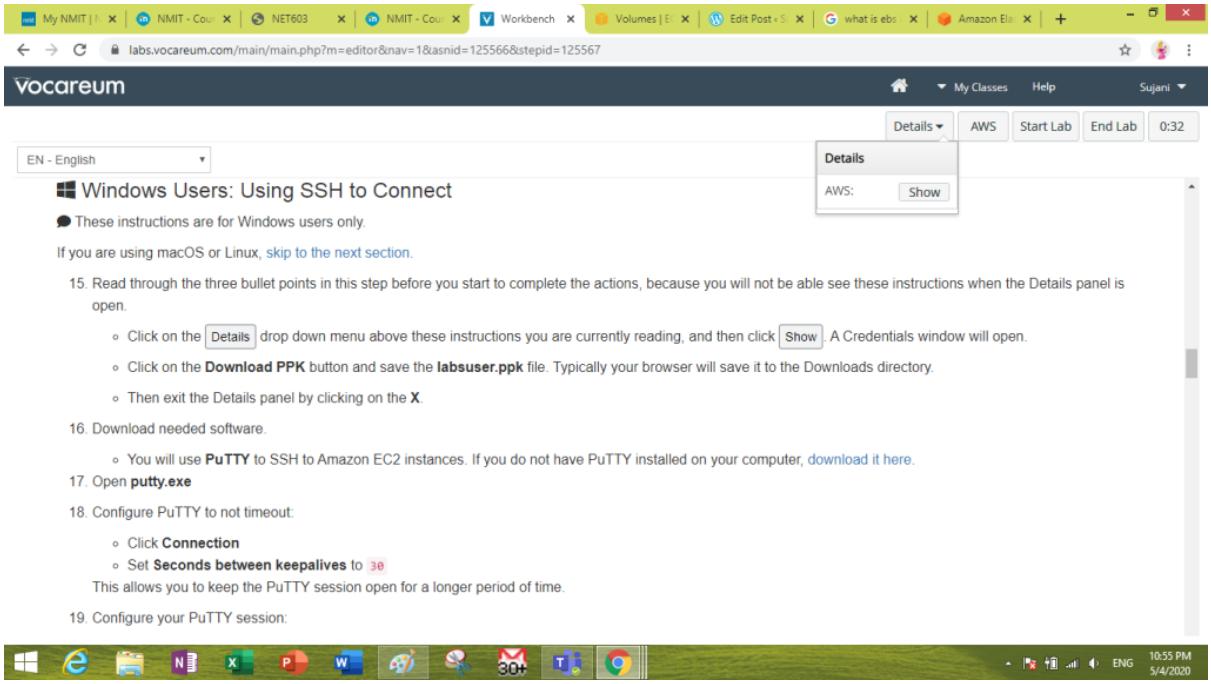


Figure 4.9 Click show

Click on the **Download PPK** button in the Credentials window–> save the **labsuser.ppk** file –> close the window –>

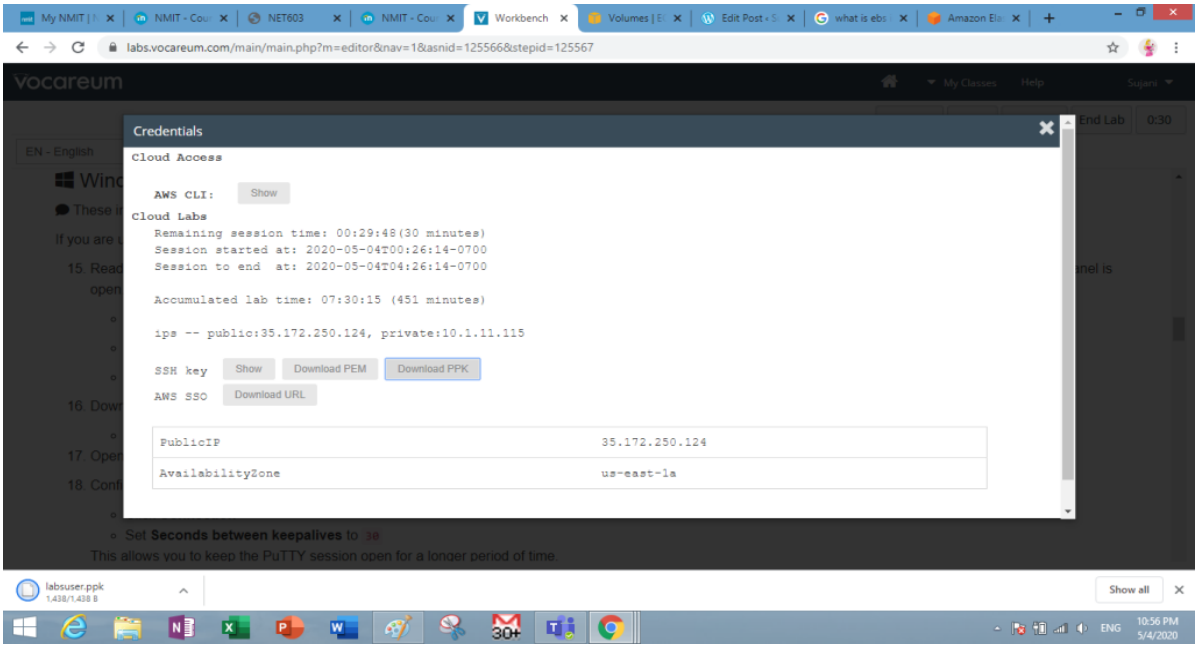


Figure 4.10

We need to install **PuTTY** to configure SSH. click the following link in our instruction page to download it.

If you do not have PuTTY installed on your computer, download it here.

Open the downloaded **putty.exe** file –> select connection –> Set **Seconds between keepalives** to 30 –>

Note: This will allows us to keep the PuTTY session open for a longer period of time.

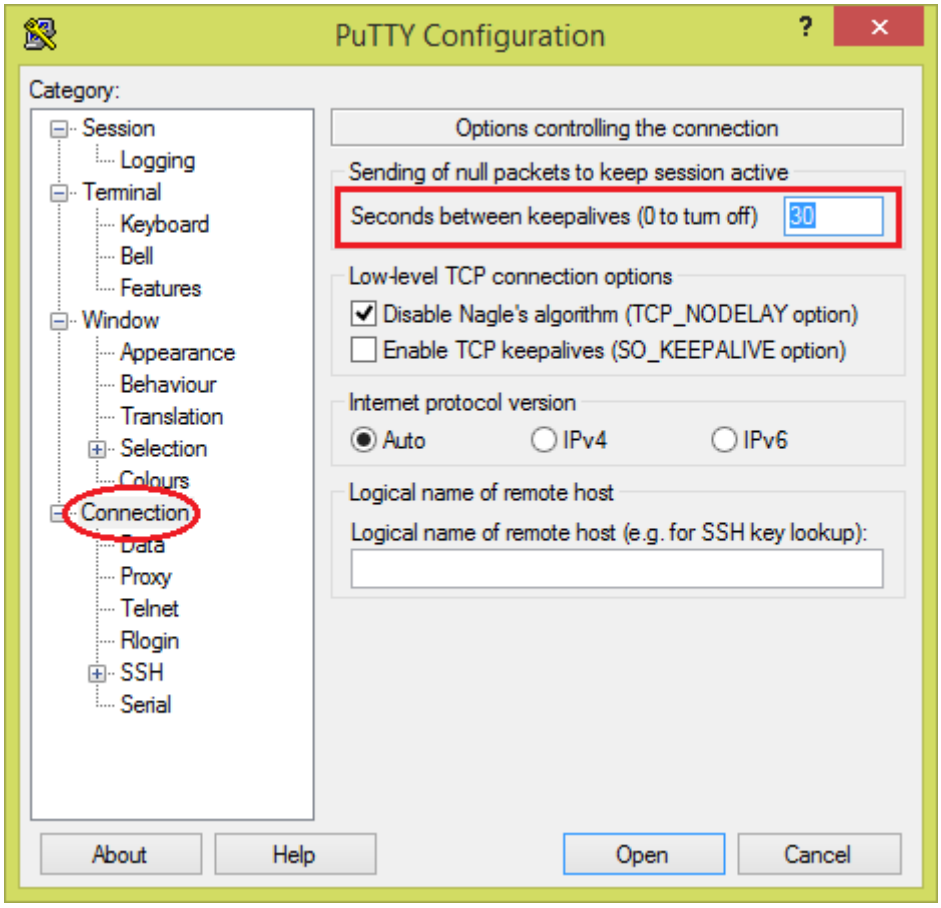


Figure 4.11 Copy and paste the IPv4 Public IP address

Click **Session** –> Copy and paste the **IPv4 Public IP address** of the instance into **Host Name (or IP address)** section –>

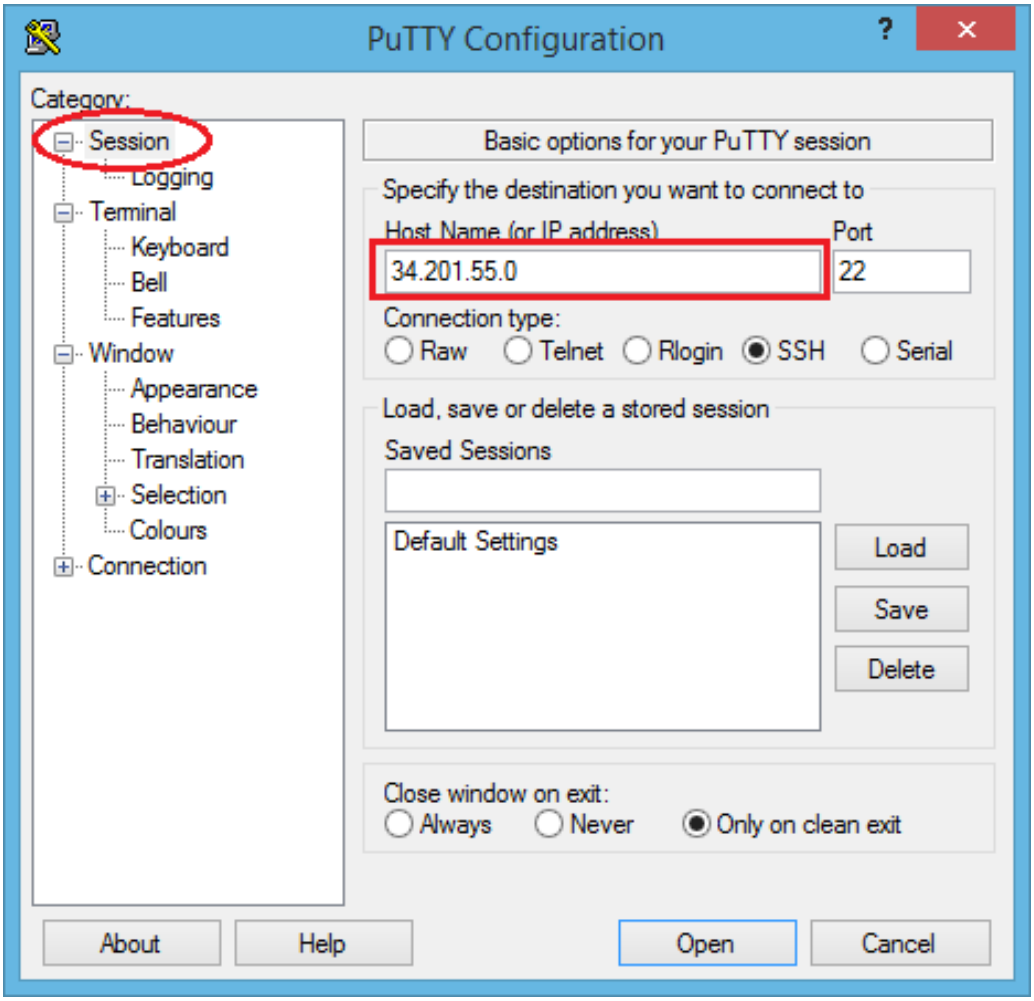


Figure 4.13

expand + **SSH** in the connection list –> Click **Auth** (don't expand it) –> Click **Browse** –> select the **labsuser.ppk** file –> Click **Open** to select it –> Click **Open** –>

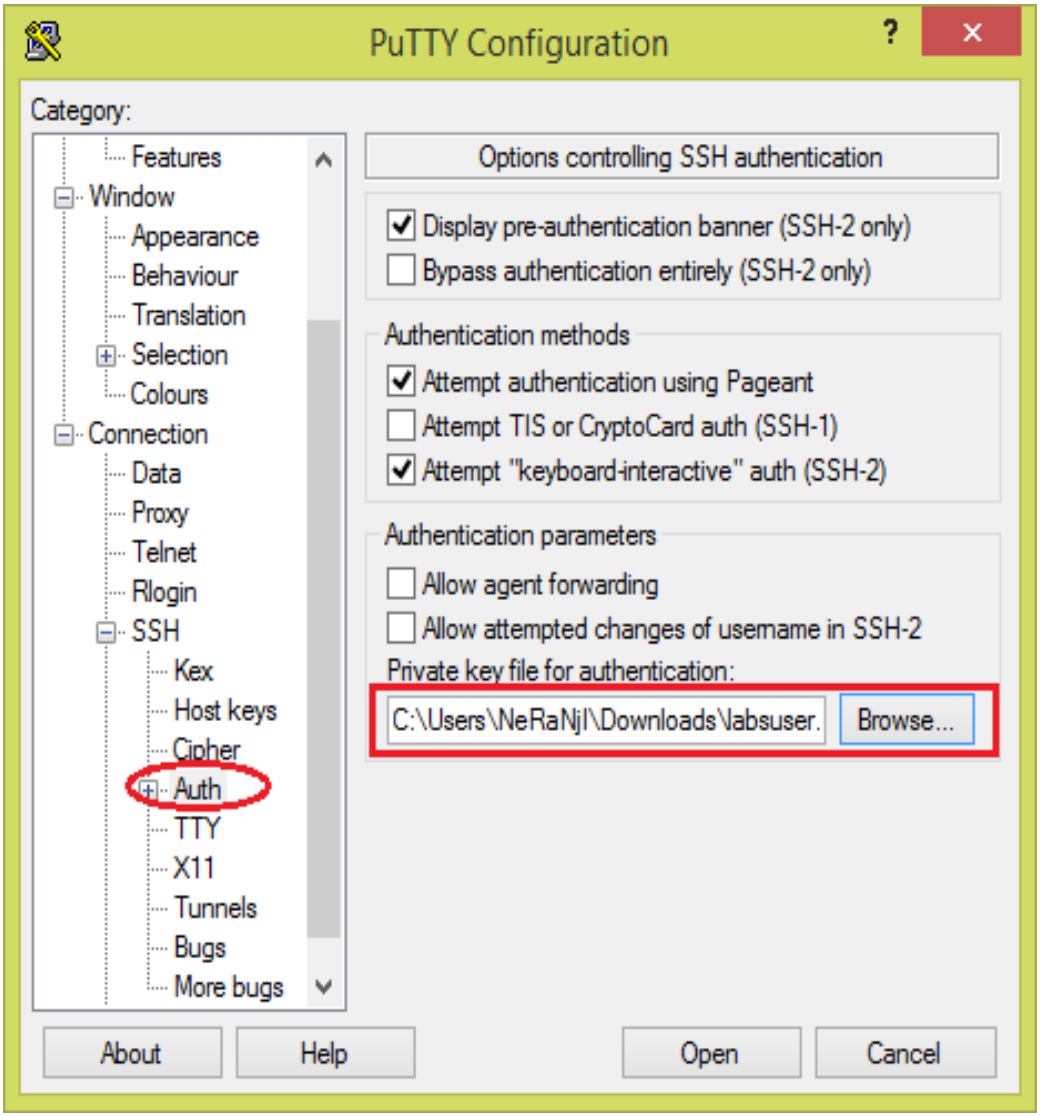


Figure 4.14 Click Yes, to trust the host and connect

Click **Yes**, to trust the host and connect

Type the login name **ec2-user** and connect to the EC2 instance named Lab –>

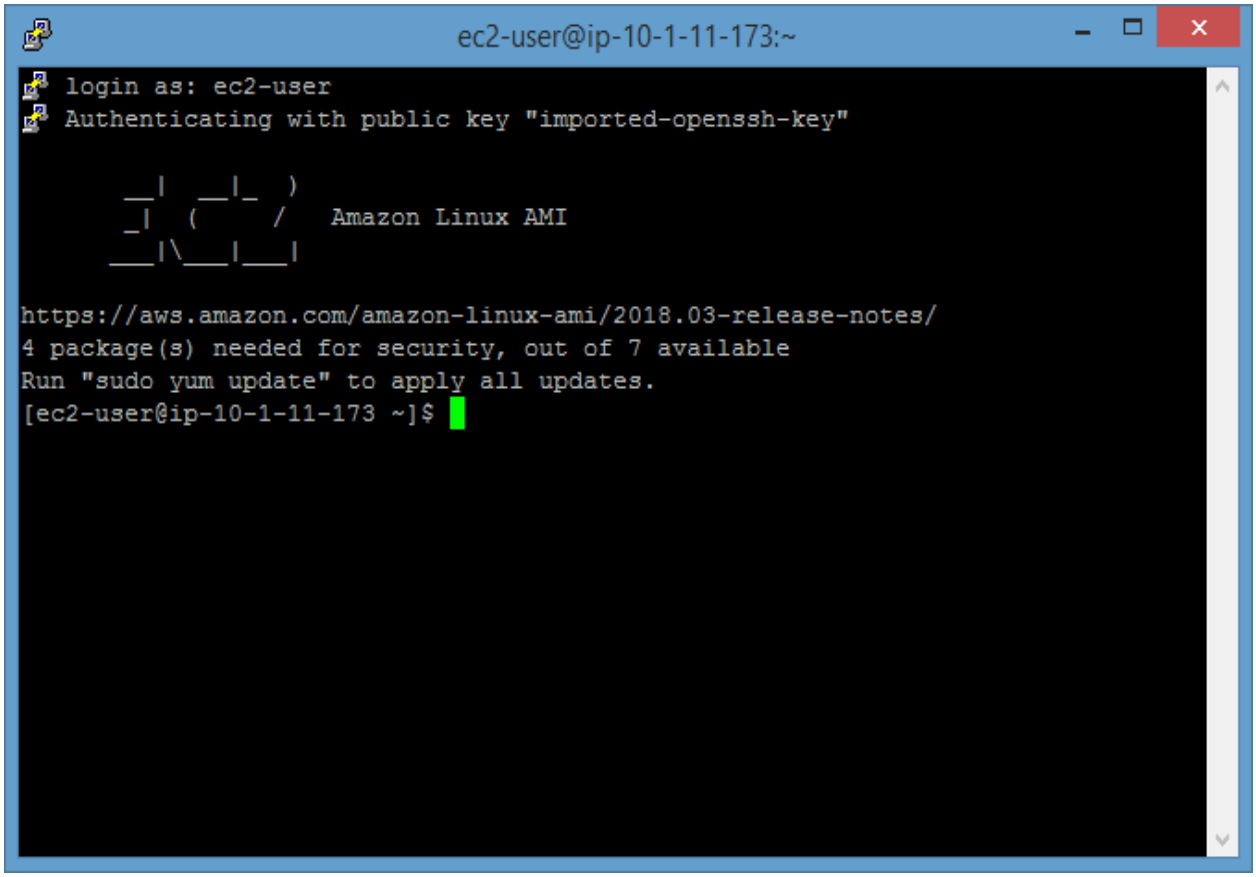


Figure 4.15

Task 4: Create and Configure Your File System

Type the following command in command line interface:

- View the available storage in the instance –**df -h**

Note: It shows only the 8GiB volume.

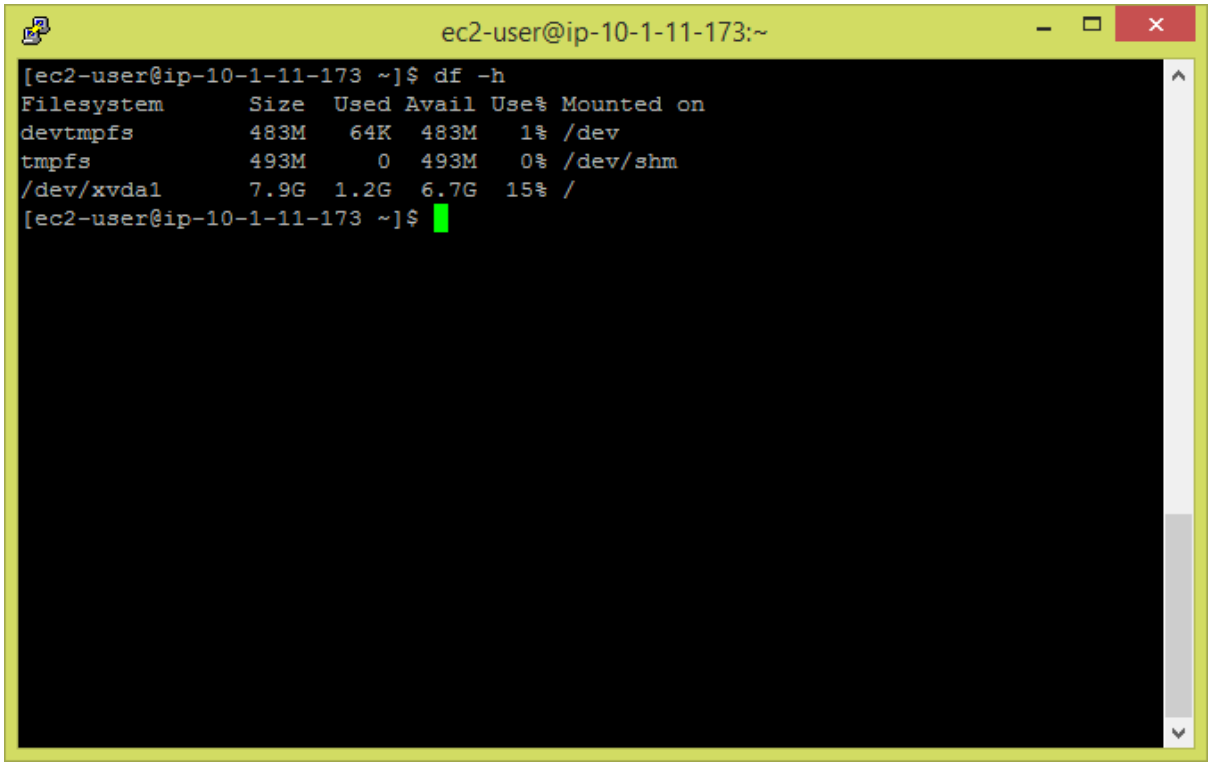


Figure 4.16

- Create an ext3 file system on the new volume – **sudo mkfs -t ext3 /dev/sdf**

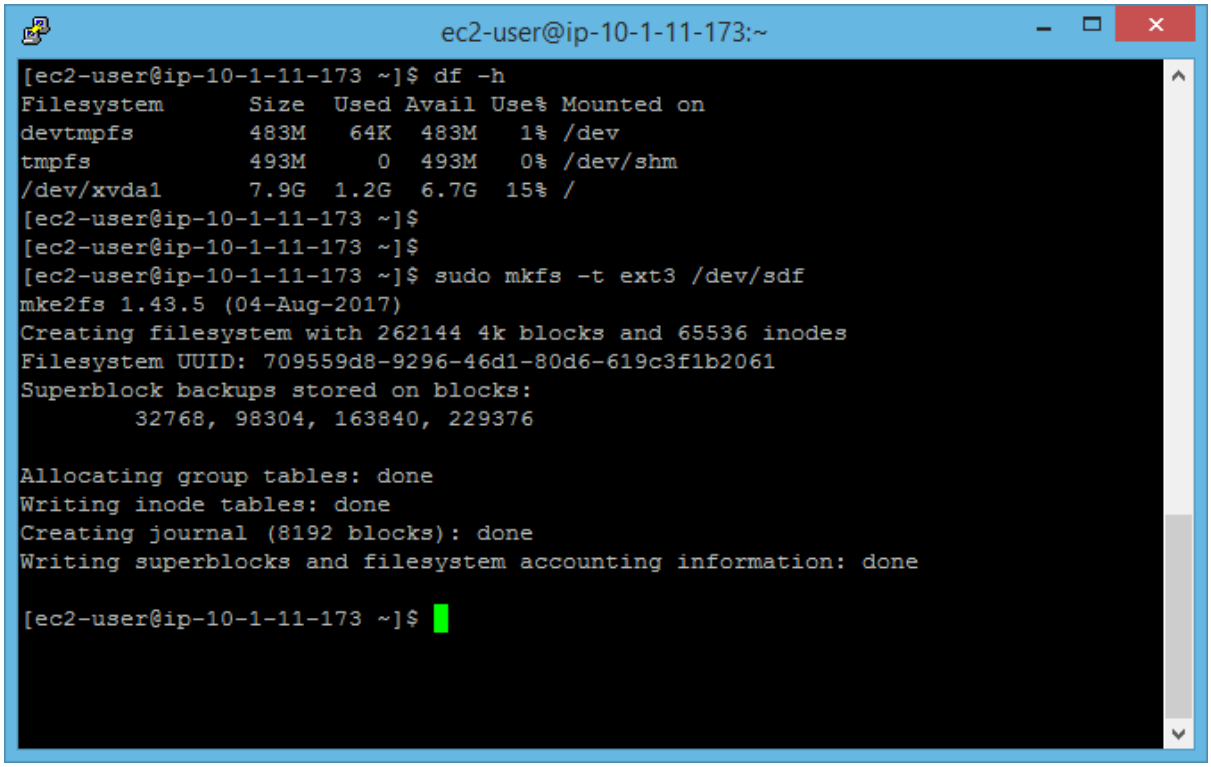


Figure 4.17

- Create a directory for mounting the new storage volume – **sudo mkdir /mnt/data-store**

- Mount the new volume – **sudo mount /dev/sdf /mnt/data-store**

Figure 4.18

- Mount this volume when the instance is started – **echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab**

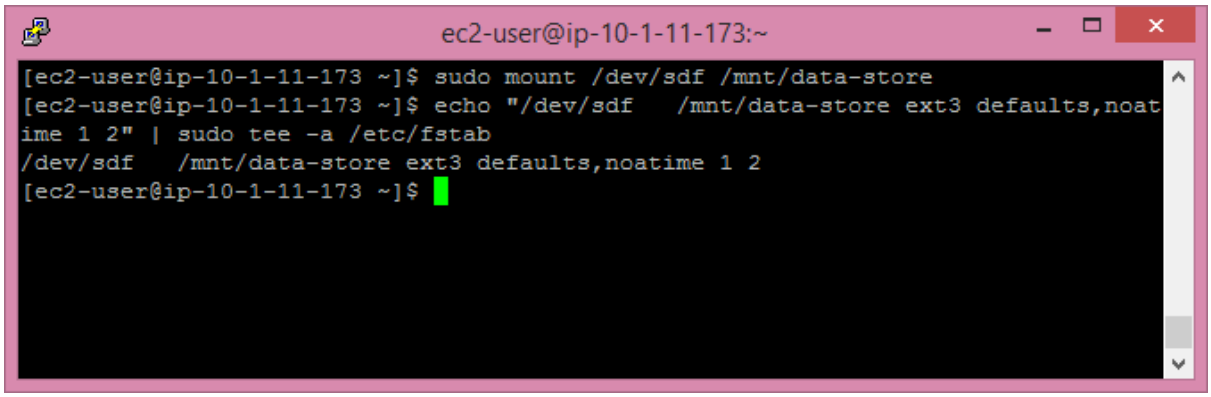


Figure 4.19

- View the configuration file to see the setting on the last line – **cat /etc/fstab**

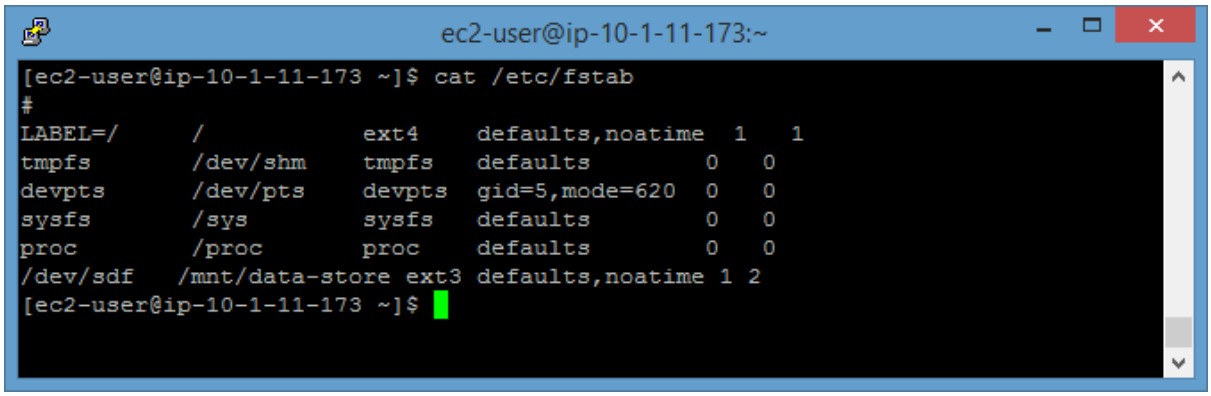


Figure 4.20

- View the available storage in the instance again –**df -h**

Note: This time we can see two volumes 8 GiB and 1 GiB

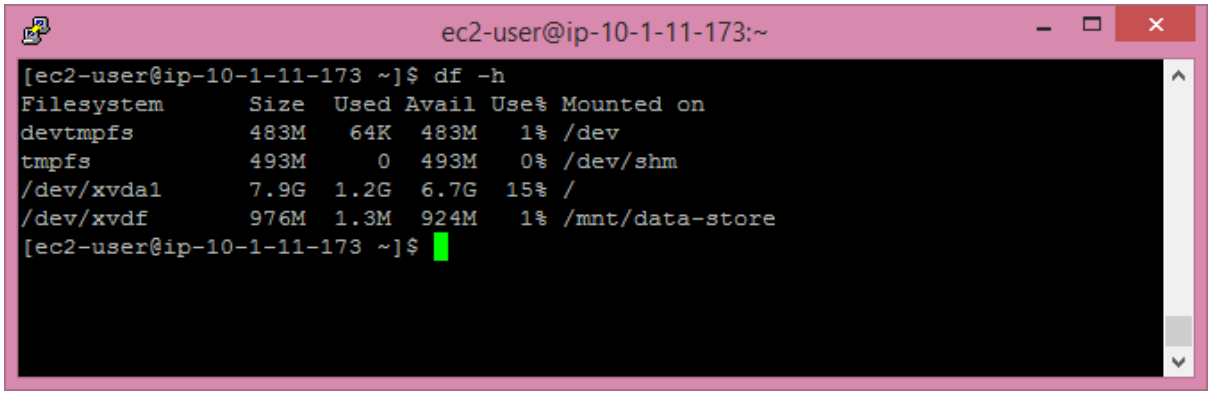


Figure 4.21

- create a file and add some text to the mounted volume – **sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"**

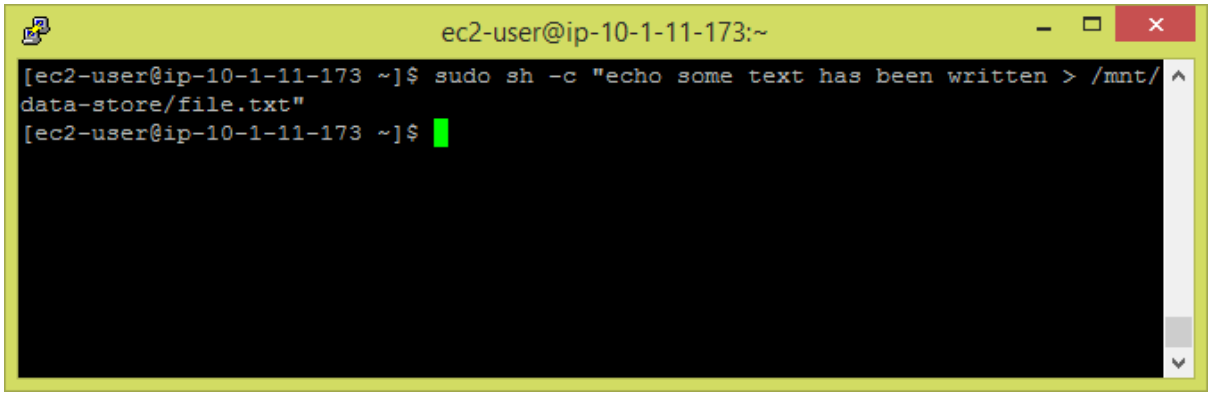


Figure 4.22

- Verify that the text has been written to the volume – **cat /mnt/data-store/file.txt**

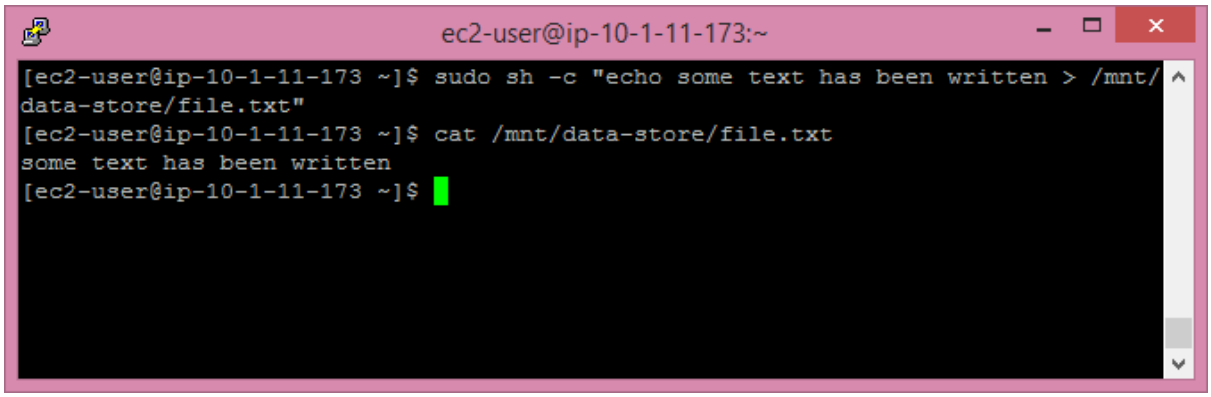


Figure 4.23

Task 5: Create an Amazon EBS Snapshot

Access the **AWS Management Console** back –> click on **Volumes** –> select **My Volume** –>

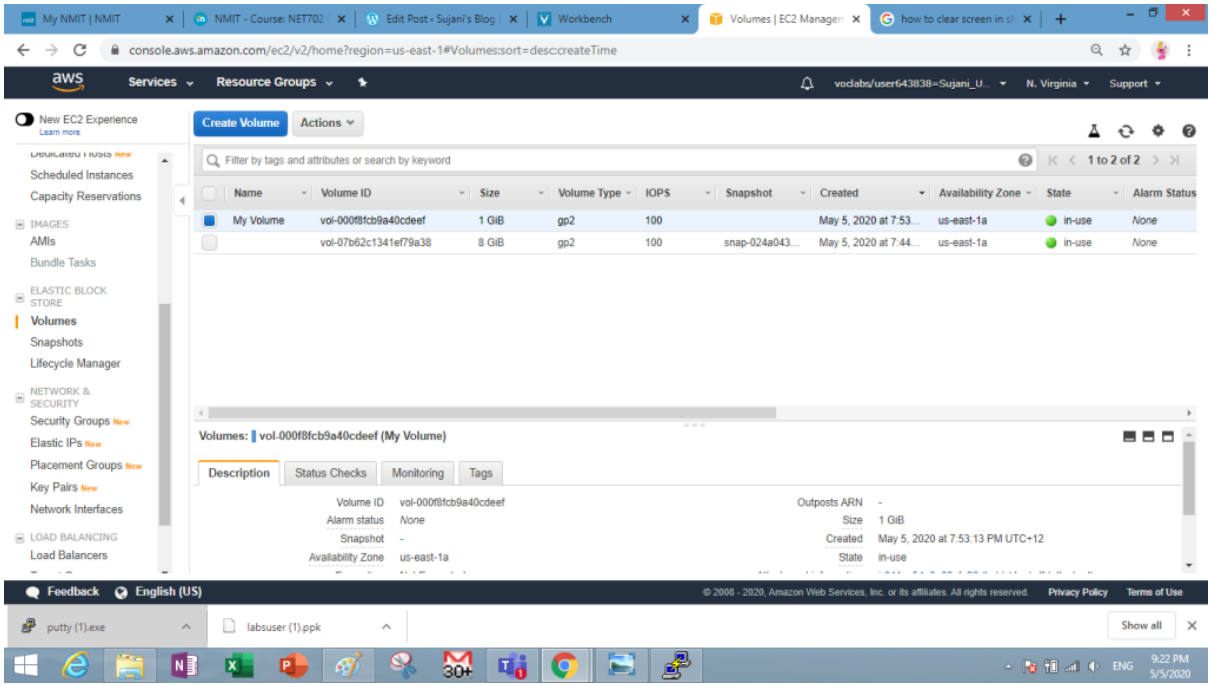


Figure 4.24

Click **Actions** menu –> click **Create Snapshot** –> Click **Add Tag** –> configure **Key:** Name –> **Value:** My Snapshot –> Click **Create Snapshot** –> click **Close** –>

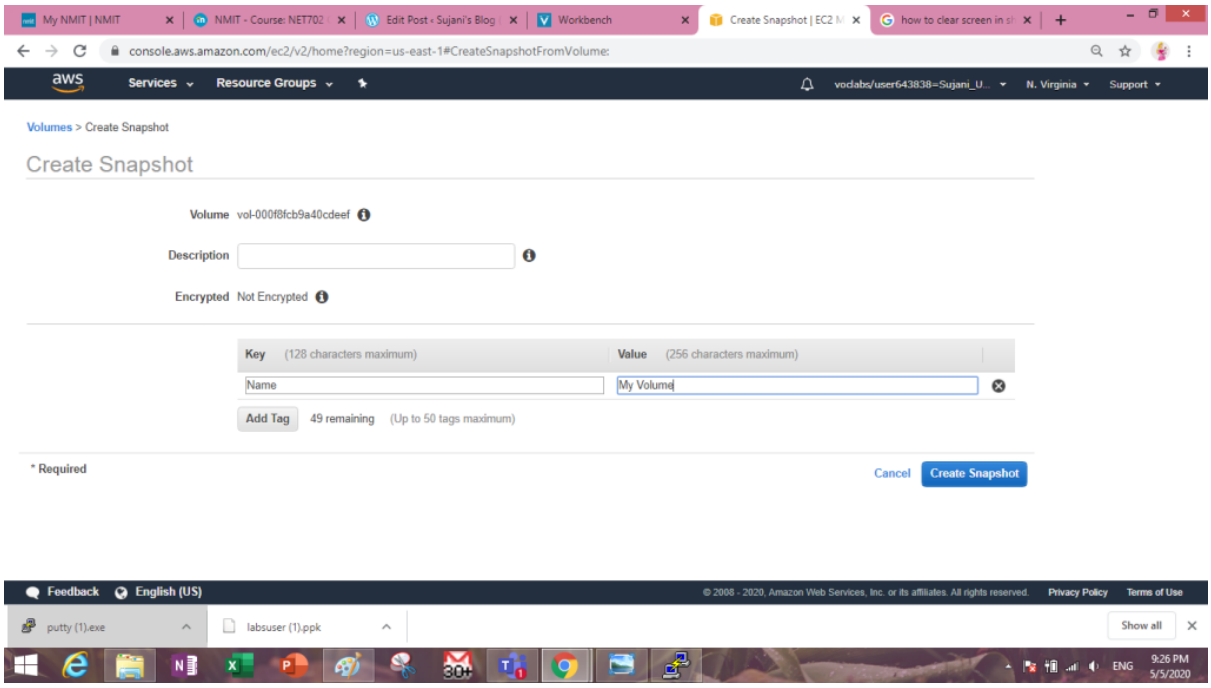


Figure 4.25

click **Snapshots** –>

Note: we can notice two status of new snapshot. Initially shows **pending** status (snapshot is being created) and change the state into **completed**. When creating snapshots of volumes, copied only used storage blocks into snapshots.

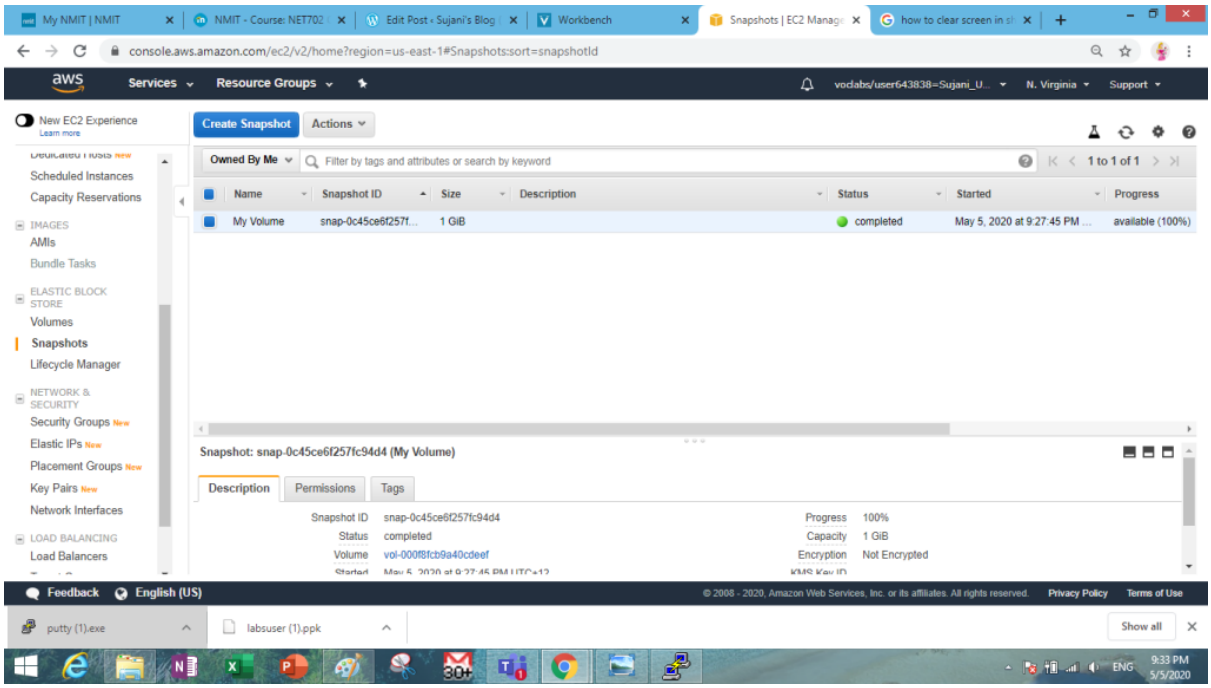


Figure 4.26

Open the SSH remote session –> enter the command **sudo rm /mnt/data-store/file.txt** for deleting the file which we created on the volume

Figure 4.27

For verifying the file has been deleted – **ls /mnt/data-store/**

Figure 4.28

Task 6: Restore the Amazon EBS Snapshot

Now we are creating a new volume using snapshot which we previously created.

Open the **AWS Management Console** –> select **My Snapshot** –> click **Create Volume** in the actions menu –> availability zone should be **us-east-1a** –>Click **Add Tag** –> select **Key:** Name –> type **Value:** Restored Volume –> Click **Create Volume** –> Click **Close** –>

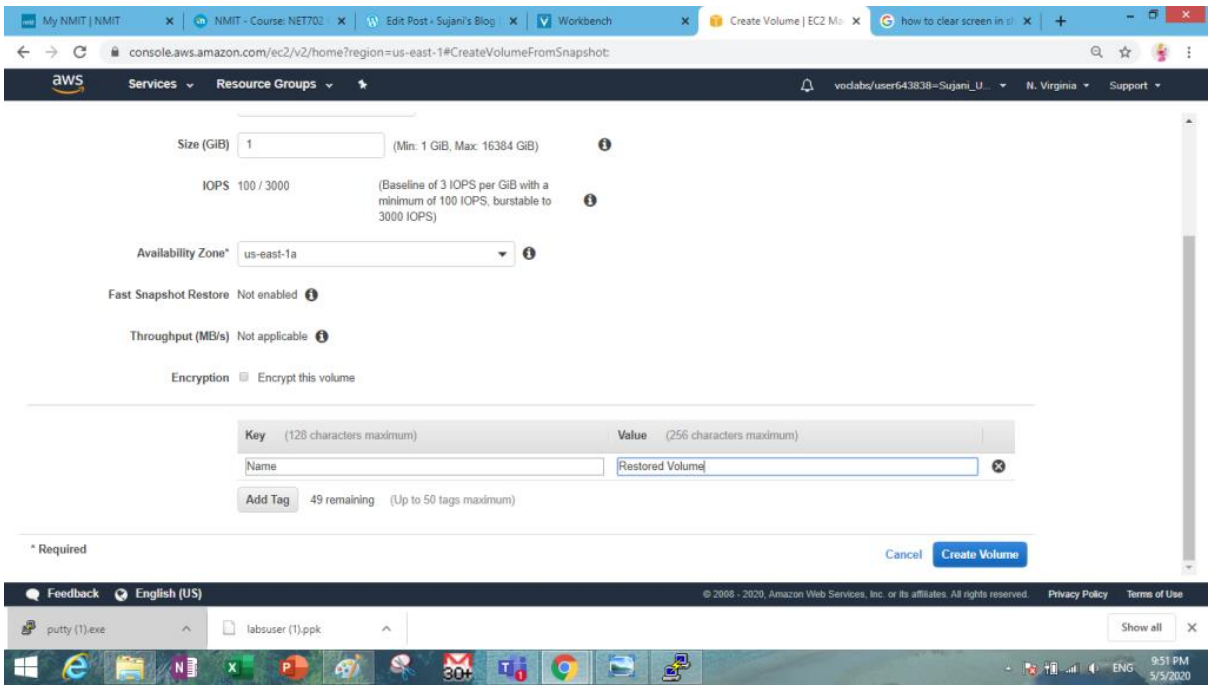


Figure 4.29

We can see three volumes in the volume list.

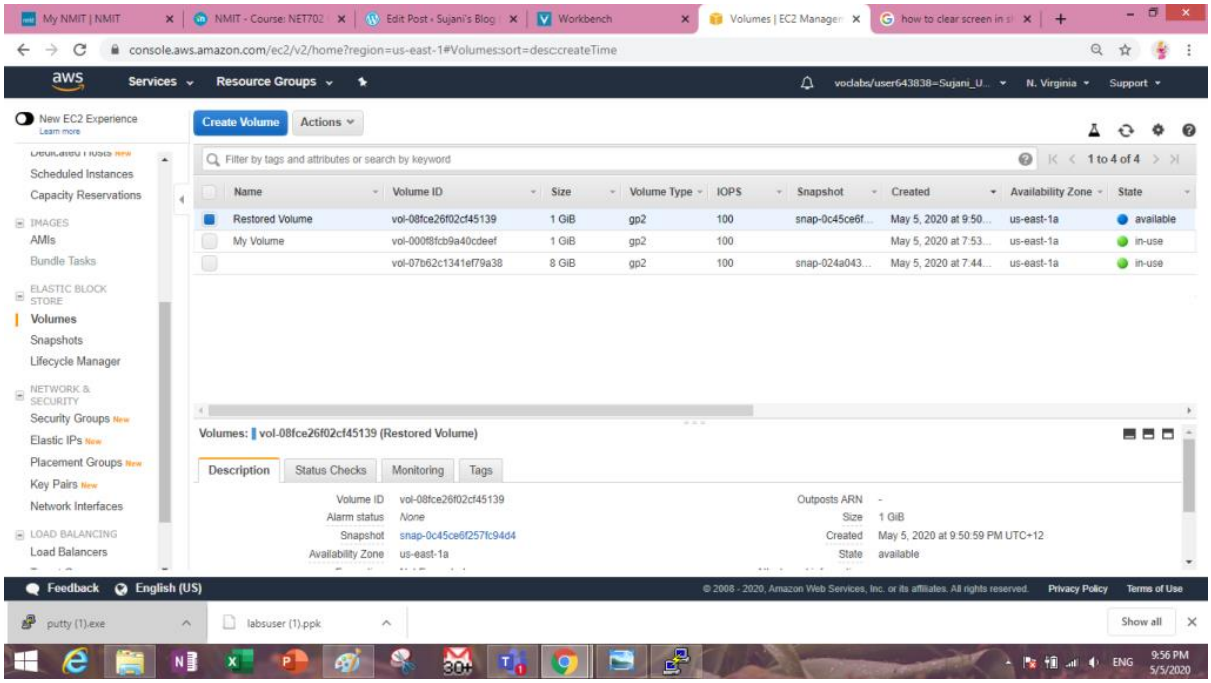


Figure 4.30

Attaching the Restored Volume to EC2 Instance

click **Volumes** –> Select **Restored Volume** –> Select the **Lab** instance in the **Instance** field –> Click **Attach** –>

Note: volume state changing from **available** to **in-use**

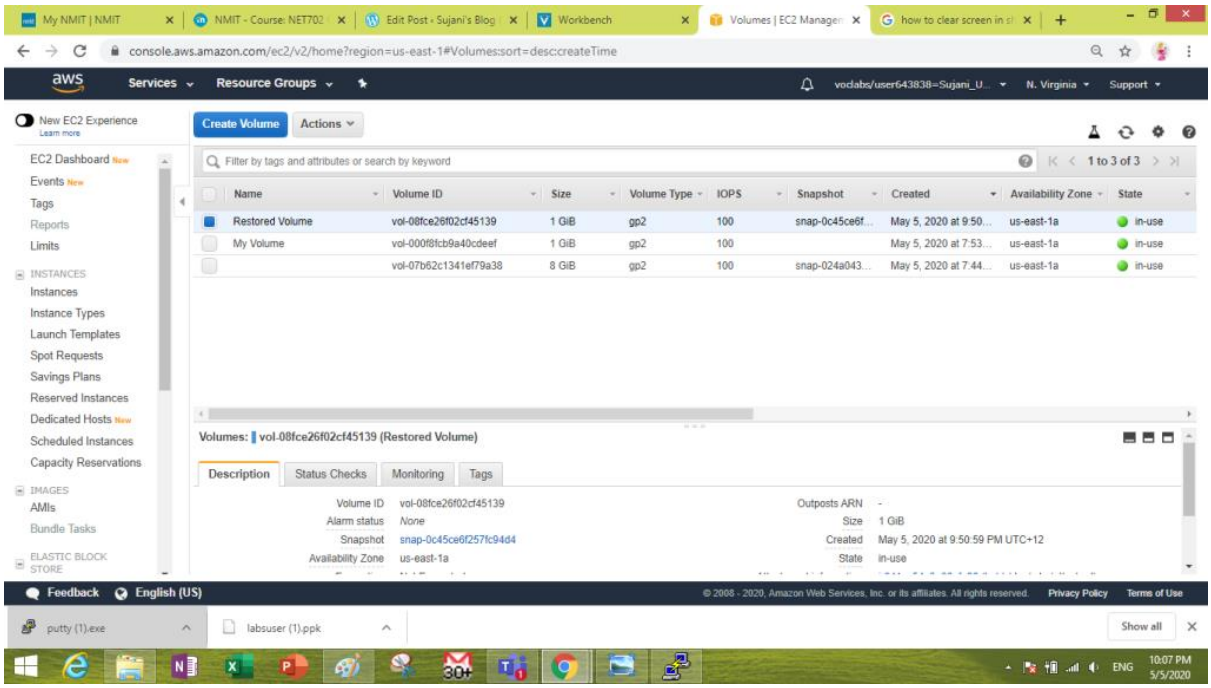


Figure 4.31

Mount the Restored Volume

Open the SSH remote session –>enter the following command for:

- Create a directory for mounting the new storage volume – **sudo mkdir /mnt/data-store2**
- Mount the new volume – **sudo mount /dev/sdg /mnt/data-store2**
- Verify that volume is mounted – **ls /mnt/data-store2/**

Figure 4.32

Result:

The experiment was successfully executed on AWS free tier in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-5

Date:

Aim: Exploring S3 bucket

Theory: First, you need to create an Amazon S3 bucket where you will store your objects.

1. Sign in to the preview version of the AWS Management Console.
2. Under **Storage & Content Delivery**, choose **S3** to open the Amazon S3 console.

If you are using the **Show All Services** view, your screen looks like this:

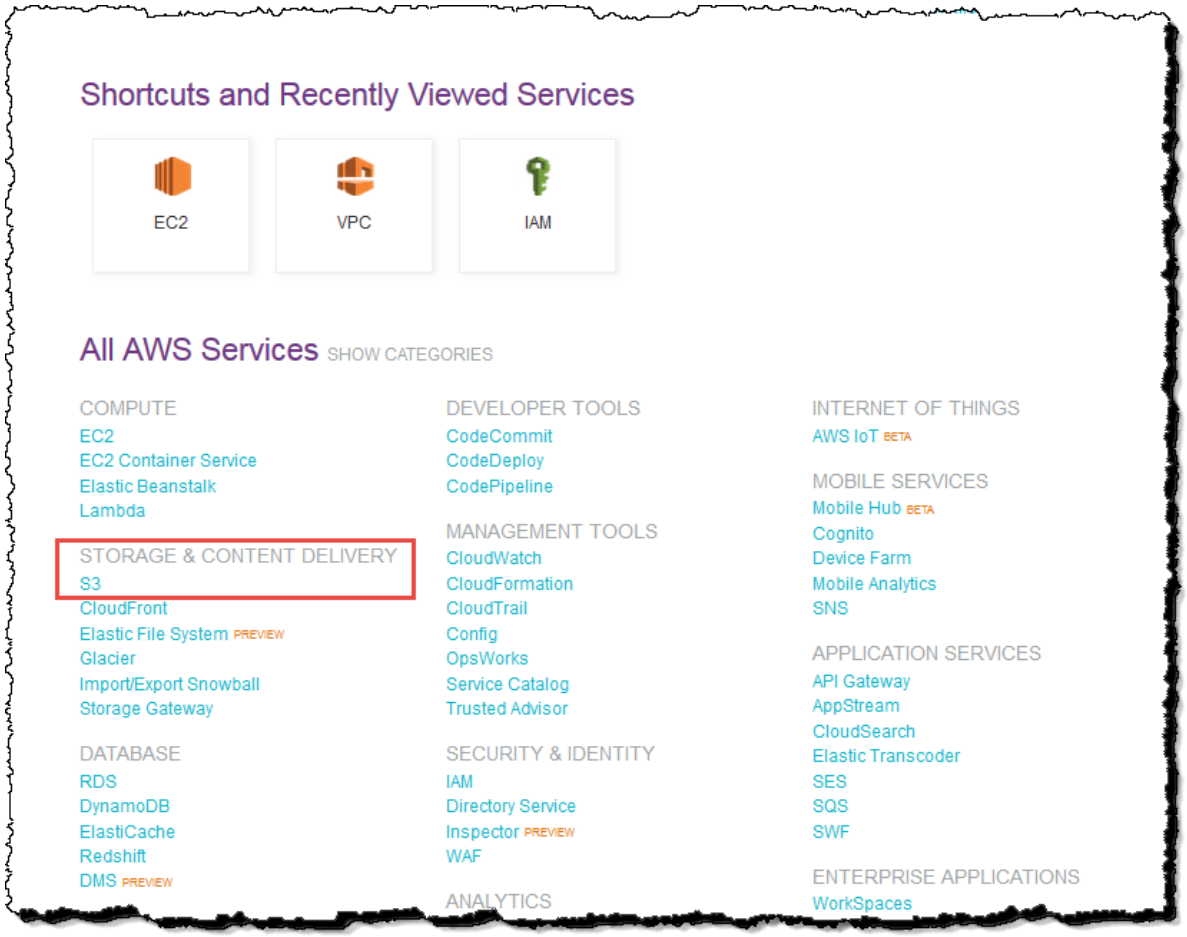


Figure 5.1

If you are using the **Show Categories** view, your screen looks like this with **Storage & Content Delivery** expanded:

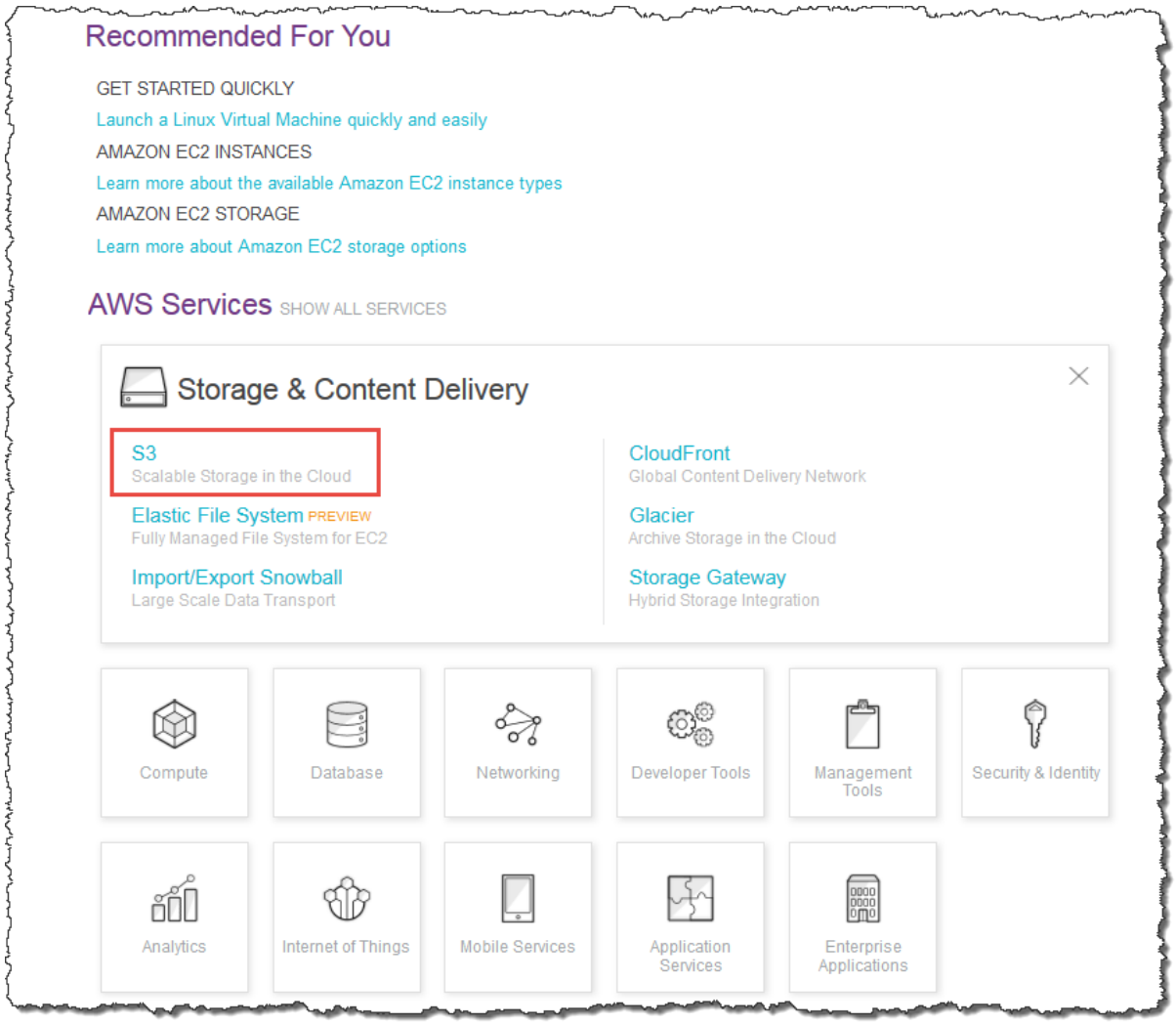


Figure 5.2

3. From the Amazon S3 console dashboard, choose **Create Bucket**.
4. In **Create a Bucket**, type a bucket name in **Bucket Name**.

The bucket name you choose must be globally unique across all existing bucket names in Amazon S3 (that is, across all AWS customers). For more information, see Bucket Restrictions and Limitations.

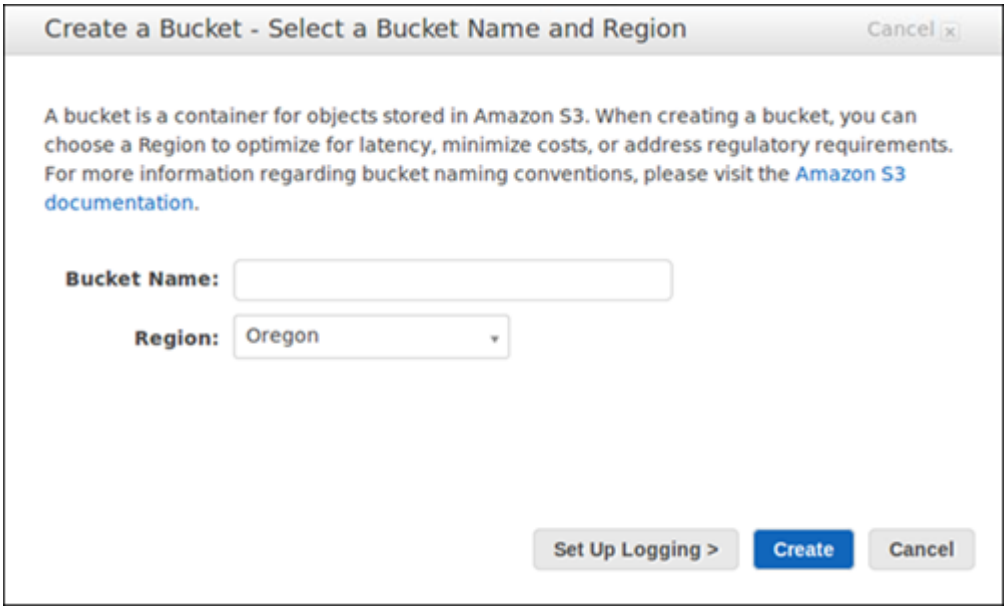


Figure 5.3

5. In **Region**, choose **Oregon**.
6. Choose **Create**.

When Amazon S3 successfully creates your bucket, the console displays your empty bucket in the **Buckets** pane.

Step 2: Upload a File to Your Amazon S3 Bucket

Now that you've created a bucket, you're ready to add an object to it. An object can be any kind of file: a document, a photo, a video, a music file, or other file type.

1. In the Amazon S3 console, choose the bucket where you want to upload an object, choose **Upload**, and then choose **Add Files**.

Figure 5.4

2. In the file selection dialog box, find the file that you want to upload, choose it, choose **Open**, and then choose **Start Upload**.

You can watch the progress of the upload in the **Transfer** pane.

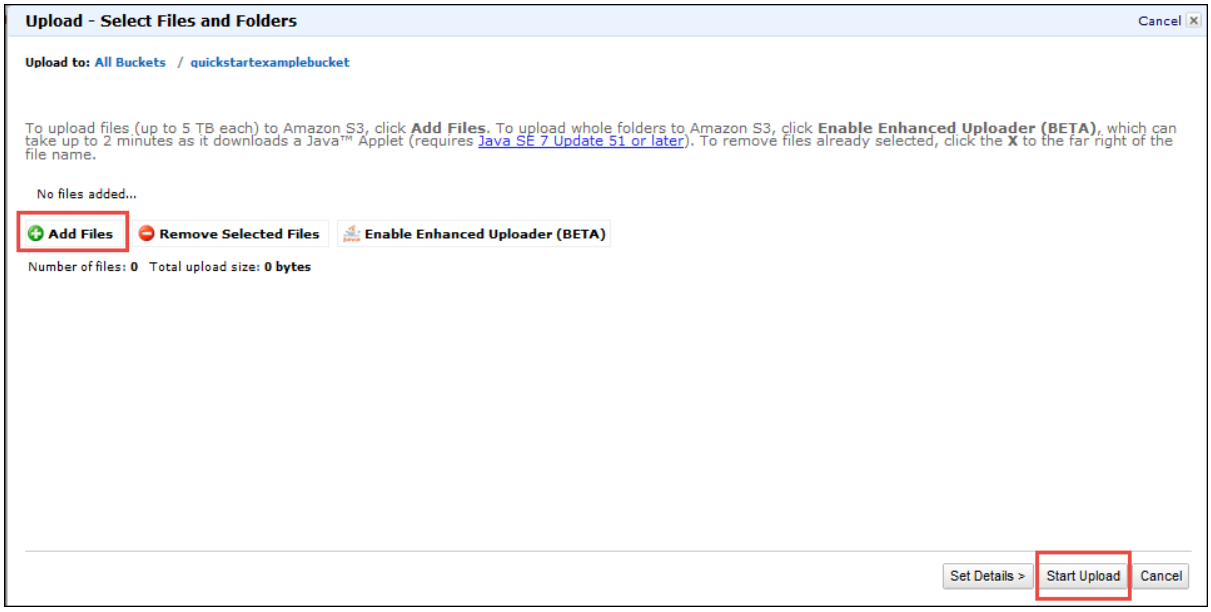


Figure 5.5

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-6

Date:

Aim: Build your VPC and launch a Web Server

Theory: In this lab, you will use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to produce a customized network. You will also create security groups for your EC2 instance. You will then configure and customize an EC2 instance to run a web server and launch it into the VPC.

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS. You can create a VPC that spans multiple Availability Zones.

Lab Scenario

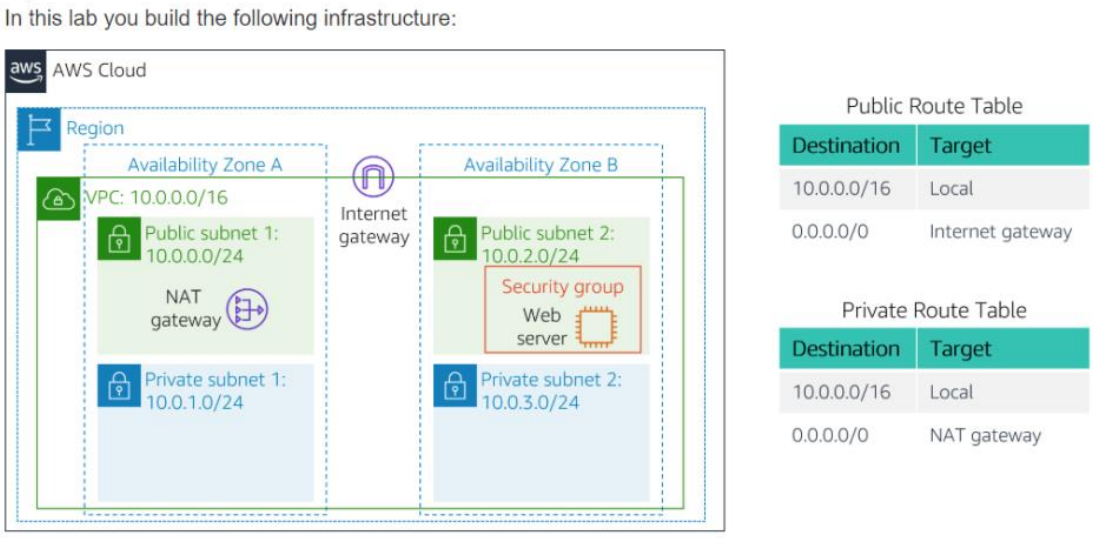
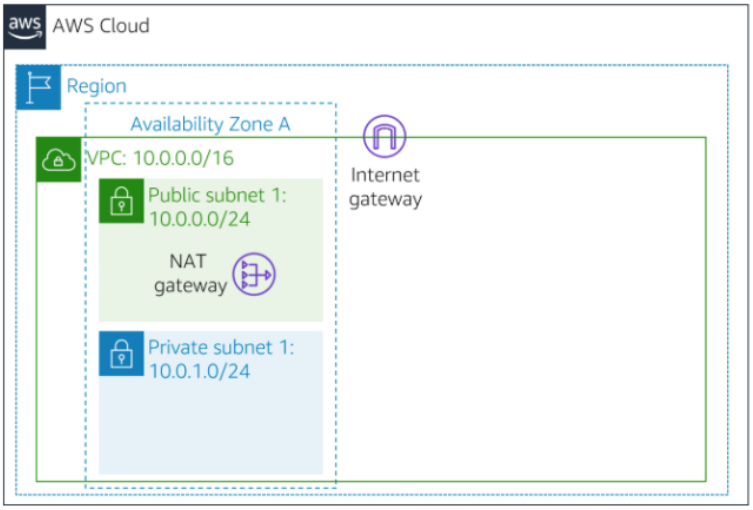


Figure 6.1

Working:

Task 1: Create Your VPC

In this task, you will use the VPC Wizard to create a VPC an Internet Gateway and two subnets in a single Availability Zone. An **Internet gateway (IGW)** is a VPC component that allows communication between instances in your VPC and the Internet.



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

The Public Subnet has a CIDR of **10.0.0.0/24**, which means that it contains all IP addresses starting with **10.0.0.x**.

The Private Subnet has a CIDR of **10.0.1.0/24**, which means that it contains all IP addresses starting with **10.0.1.x**.

Figure 6.2

In Task 1 we are going to configure VPC of first avaiblity Zone A

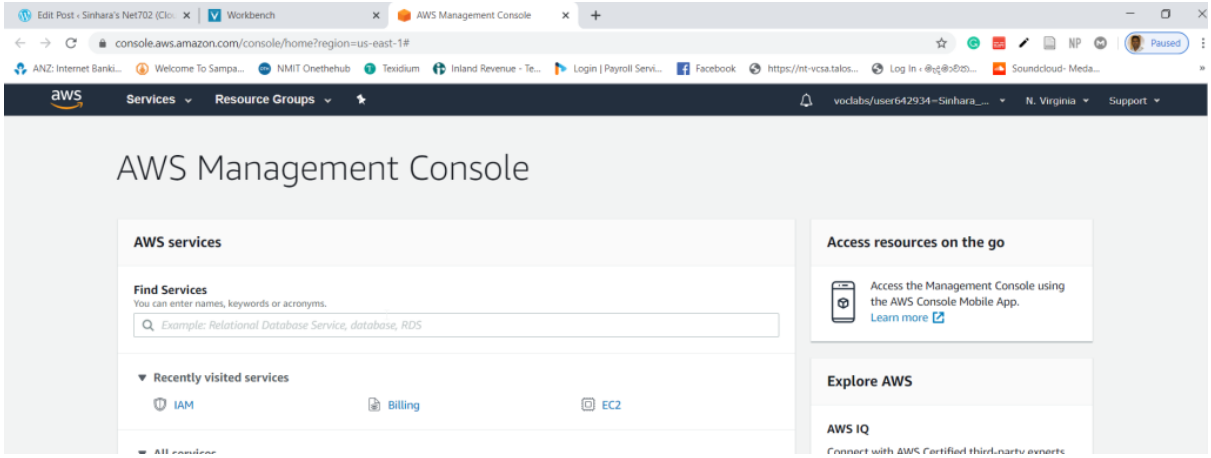


Figure 6.3

Log into the AWS Console

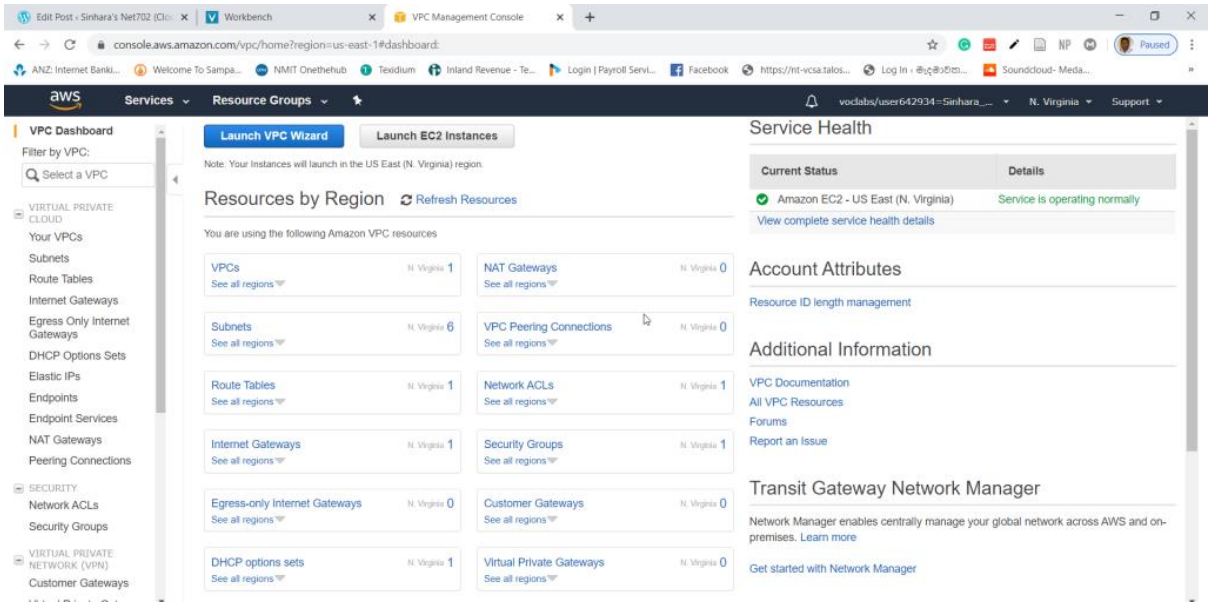


Figure 6.4

In the **AWS Management Console**, on the **Services** menu, click **VPC**.

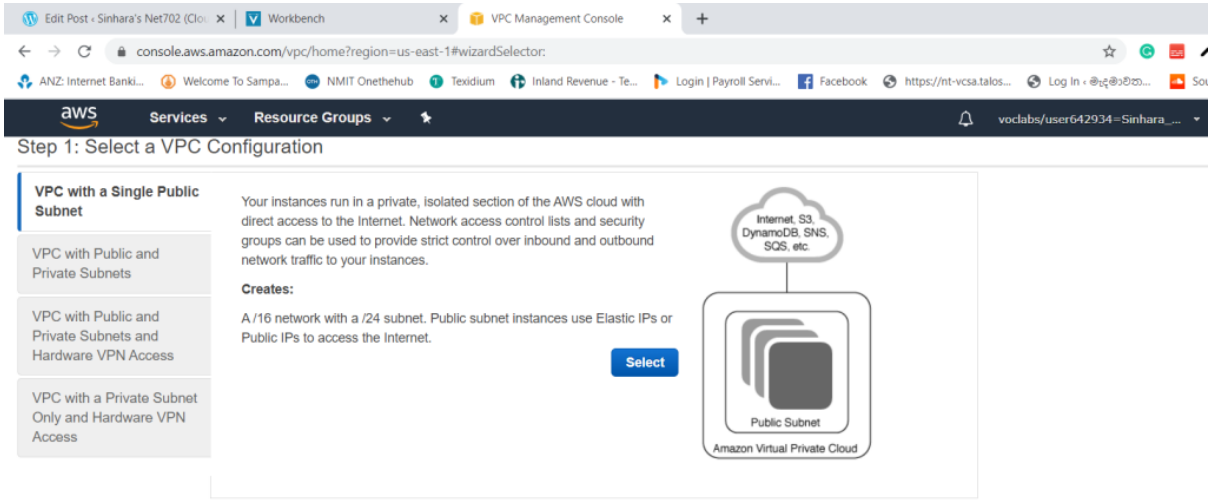


Figure 6.5

Click **Launch VPC Wizard**

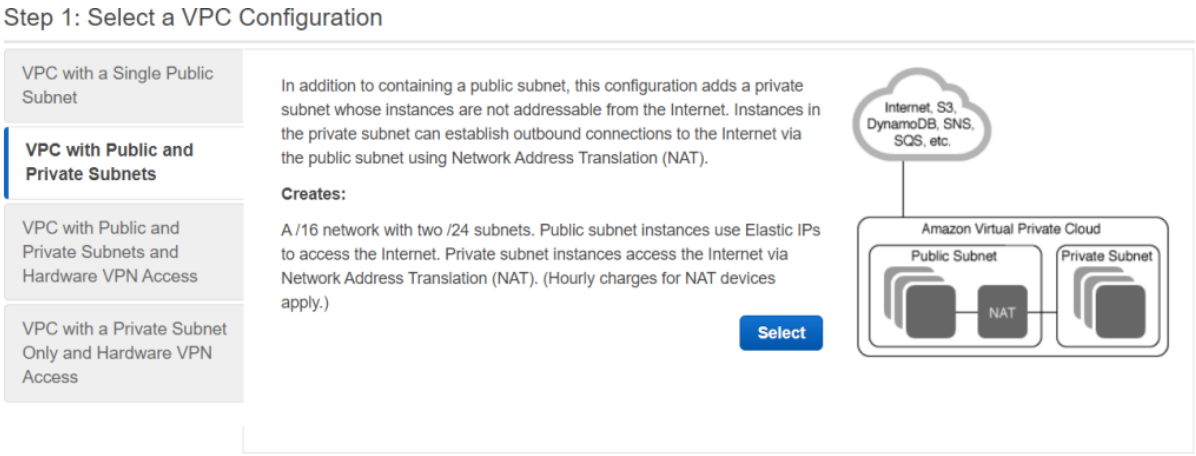


Figure 6.6

In the left navigation pane, click **VPC with Public and Private Subnets** (the second option).

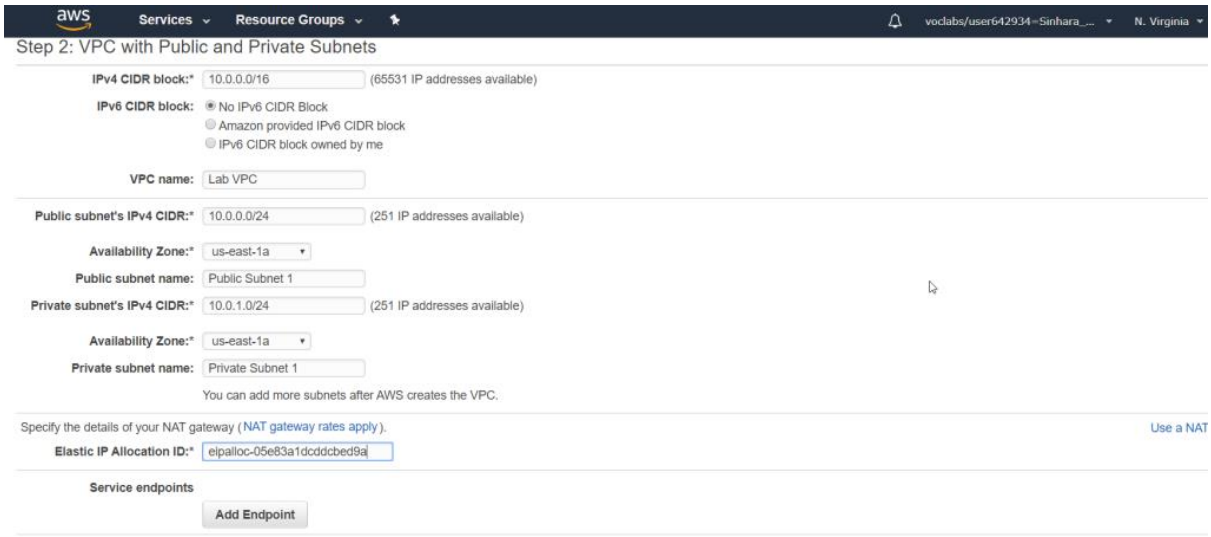


Figure 6.7

Configured VPC name,Availability Zone,Public subnet name,Private subnet name and

Elastic IP Allocation ID then created VPC

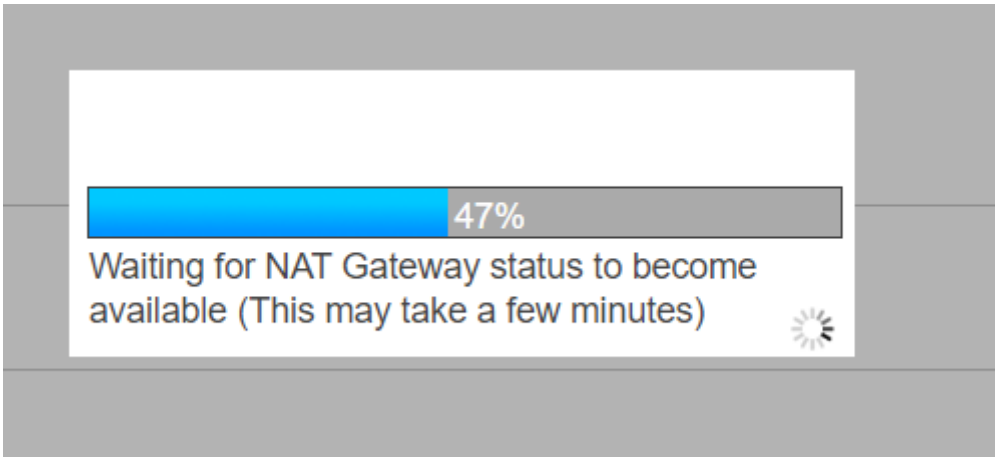


Figure 6.8

VPC creation process takes little time longer

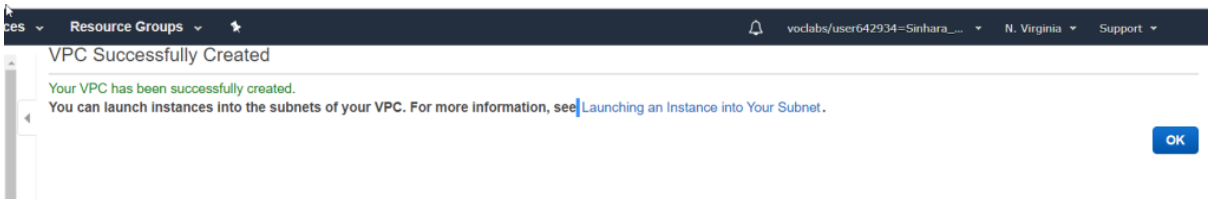


Figure 6.9

Task 2: Create Additional Subnets

In this task, you will create two additional subnets in a second Availability Zone. This is useful for creating resources in multiple Availability Zones to provide *High Availability*.

In Task 02 , we are going to configure VPC for availability Zone B

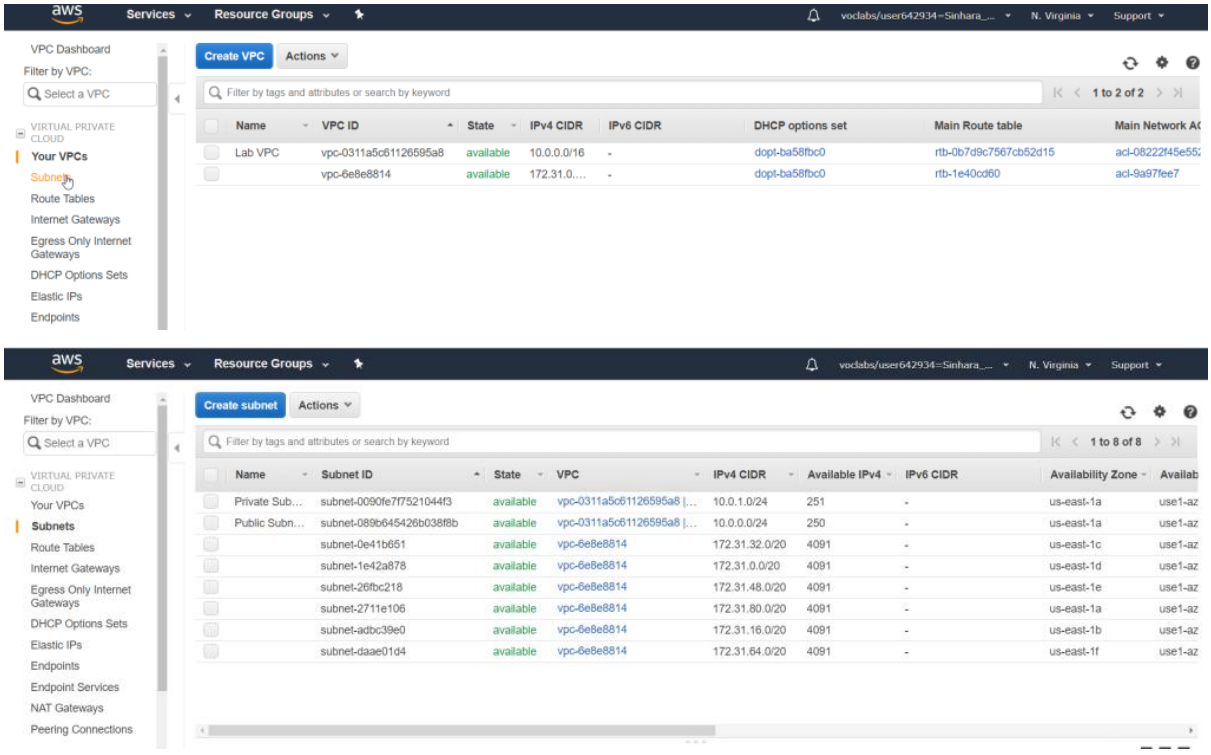


Figure 6.10

In the left navigation pane, click **Subnets**.

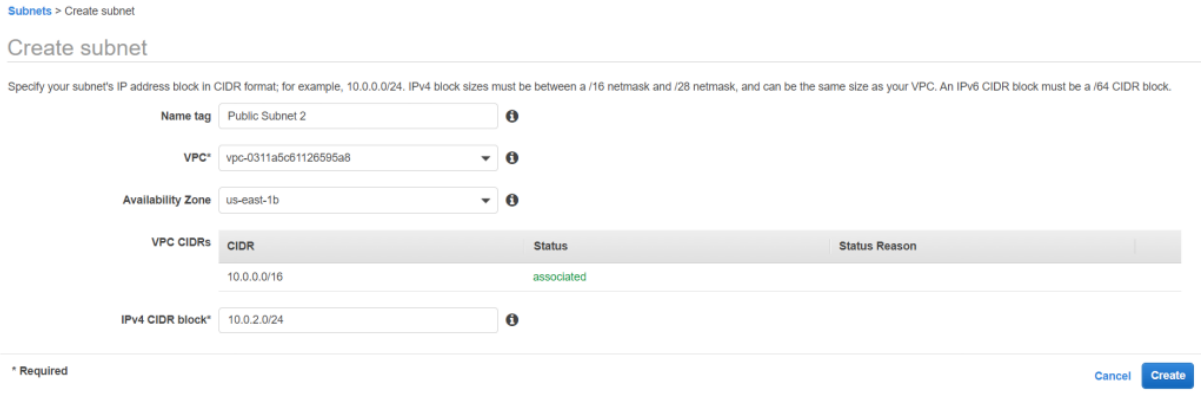


Figure 6.11

Configure second public subnet with Name tag: Public Subnet 2,VPC: Lab VPC ,second Availability Zone and

IPv4 CIDR block: 10.0.2.0/24

Figure 6.12

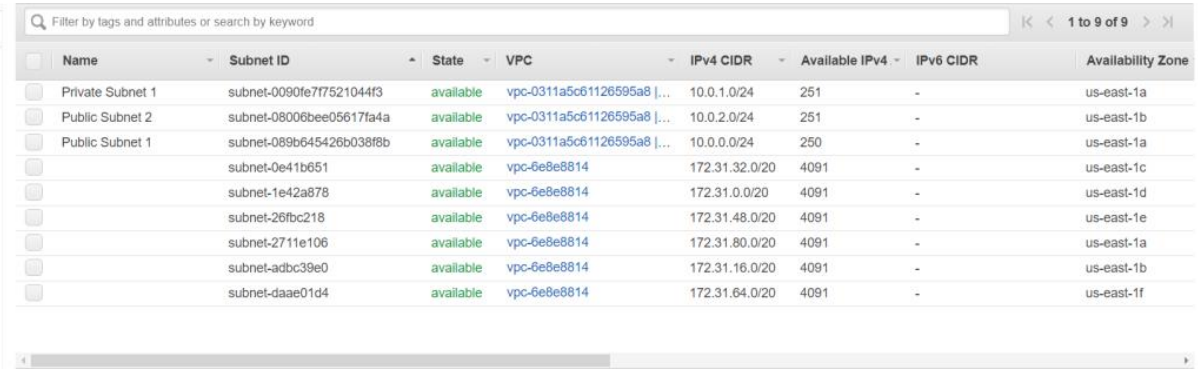


Figure 6.13

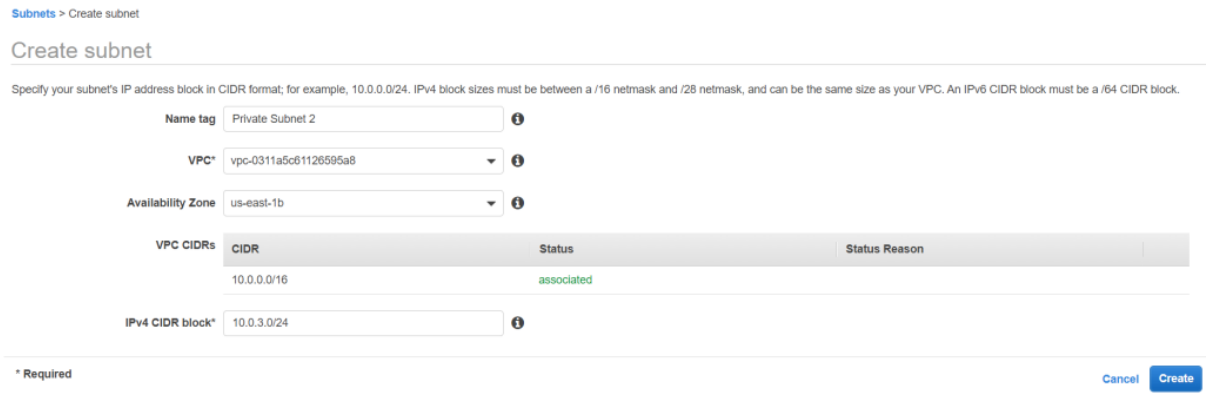


Figure 6.14

Configure second private subnet with Name tag: Private Subnet 2 ,VPC,Availability Zone, CIDR block: 10.0.3.0/24

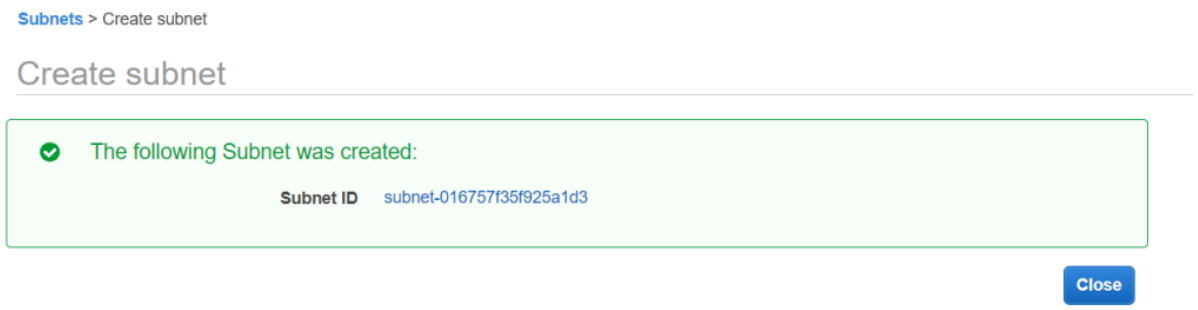


Figure 6.15

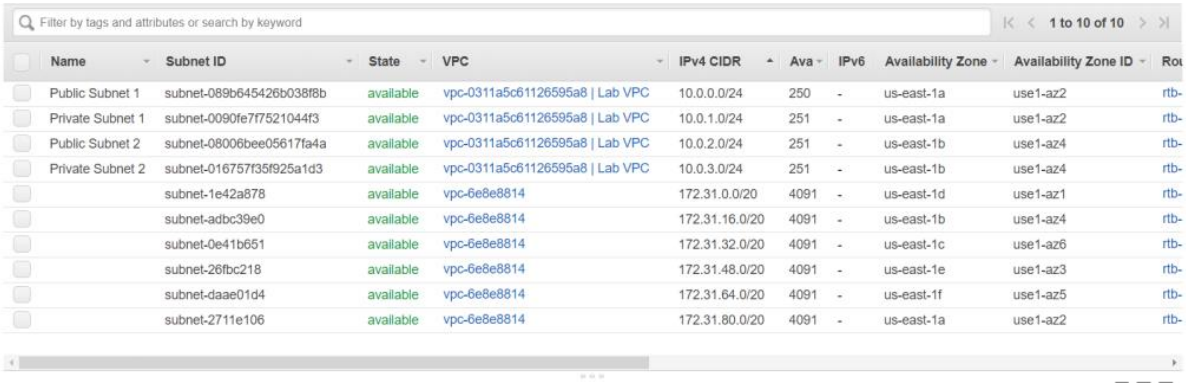


Figure 6.16

now configure the Private Subnets to route internet-bound traffic to the NAT Gateway so that resources in the Private Subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring a *Route Table*.

A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table controls routing for the subnet

Below are the steps to configure private routing table :

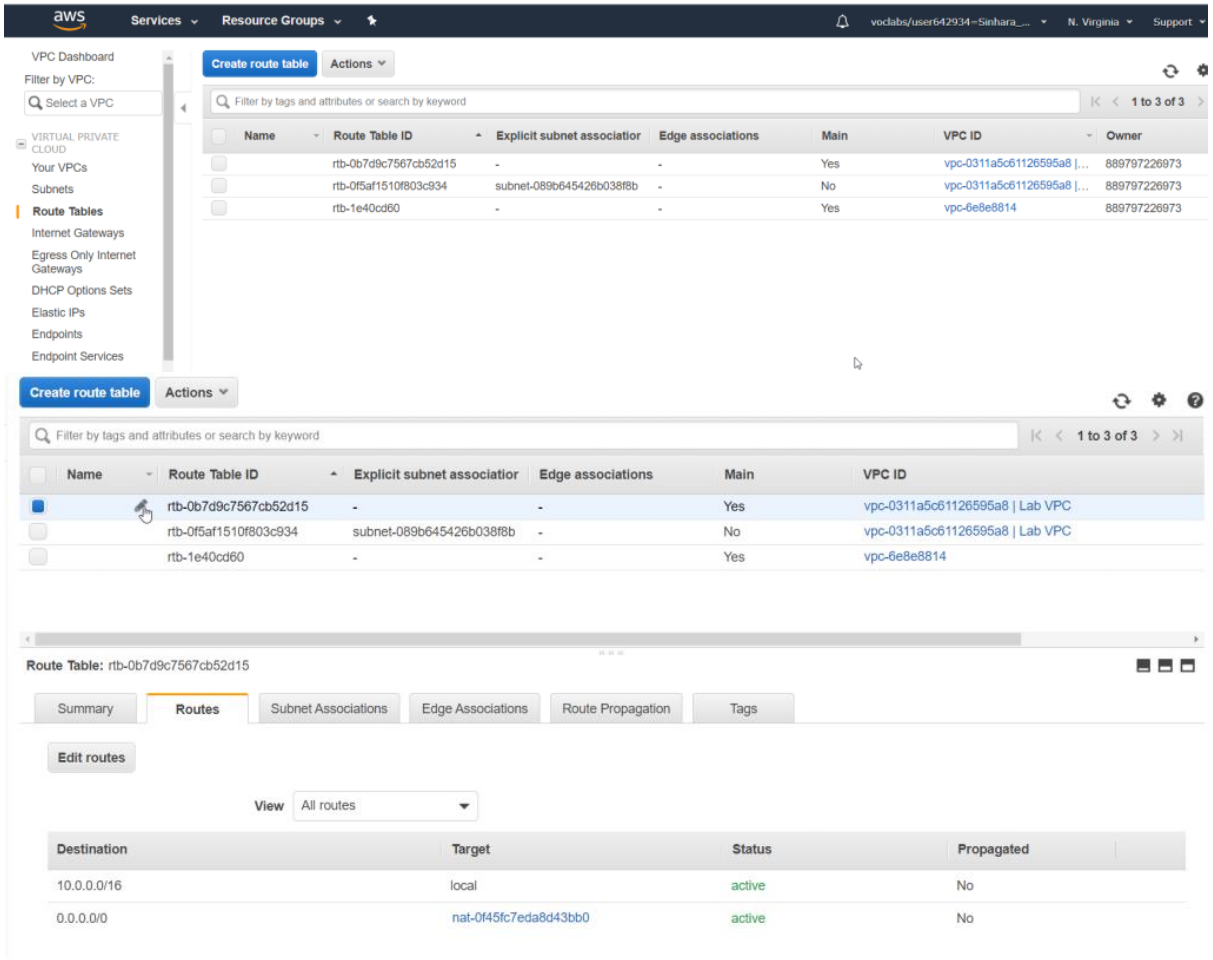


Figure 6.17

This is private routing table as we can see nat gateway device name in it for 0.0.0.0/0 destination

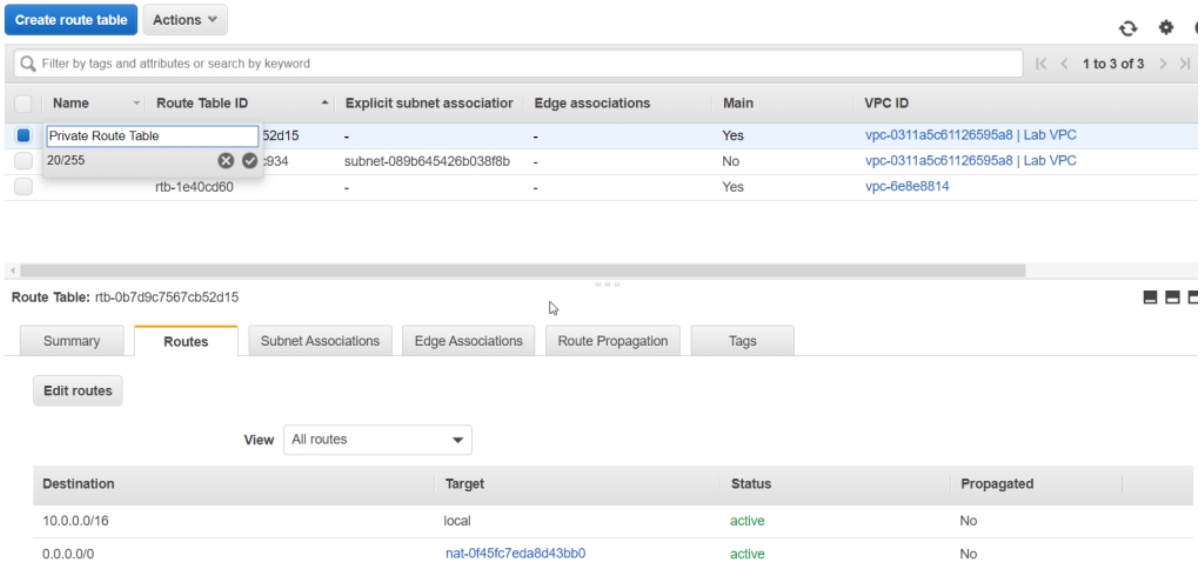
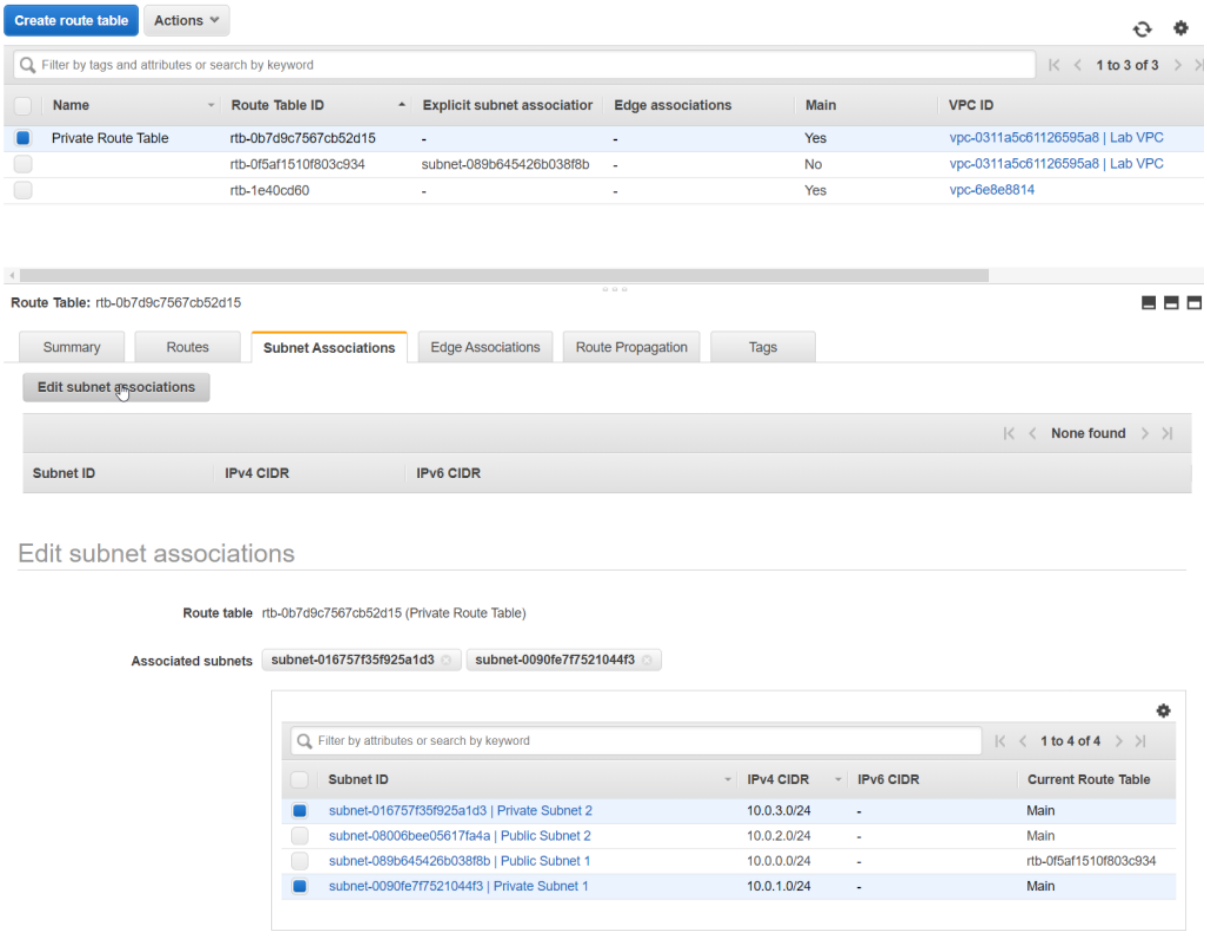
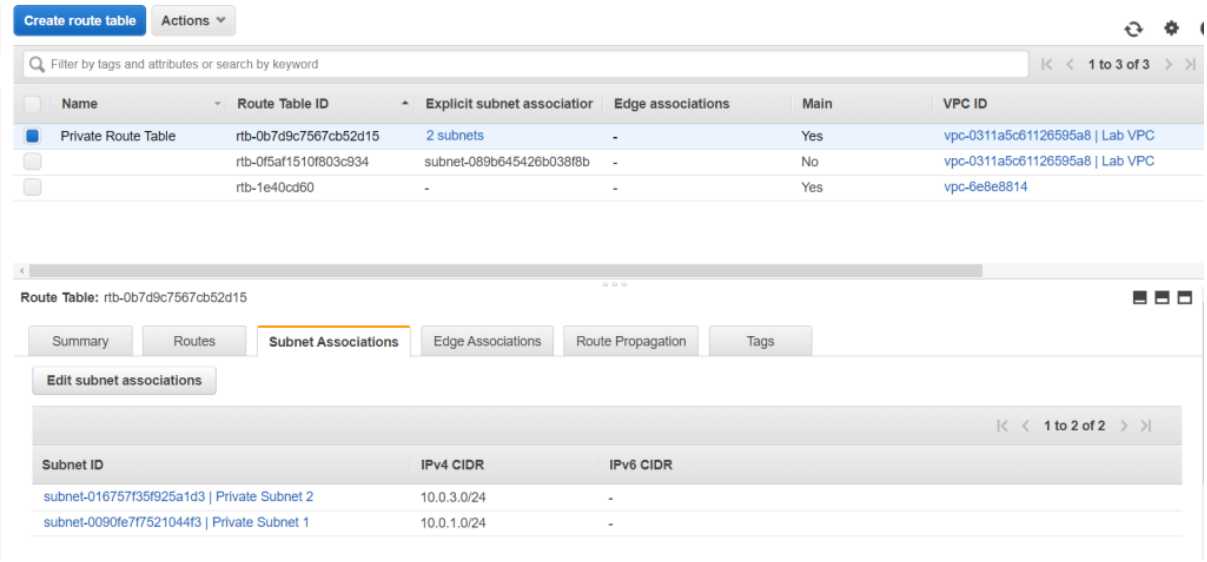


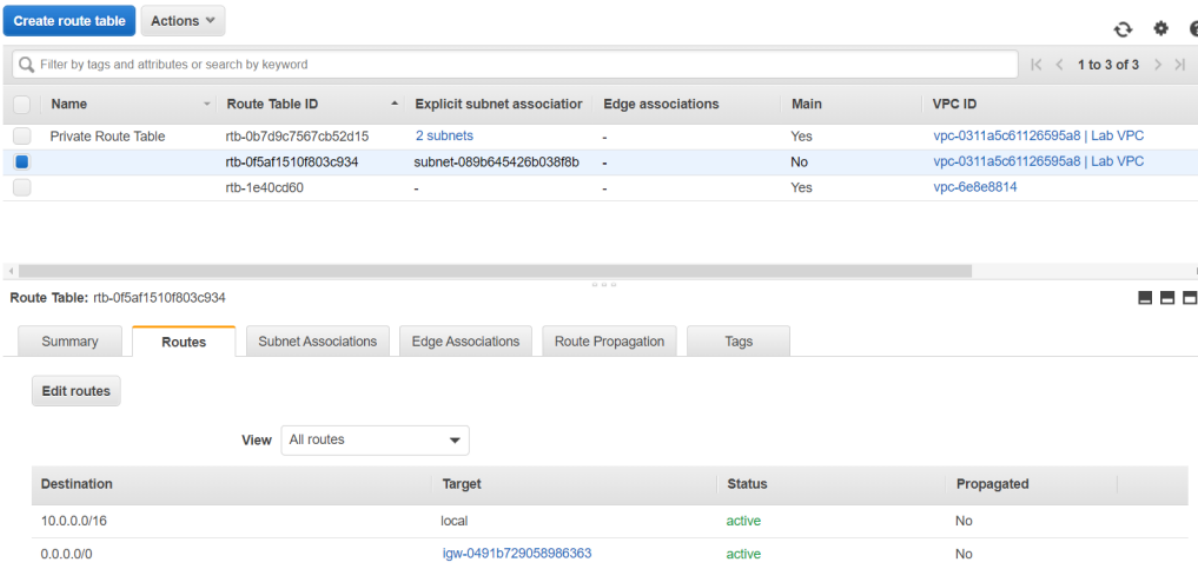
Figure 6.18 Names it as Private Route Table



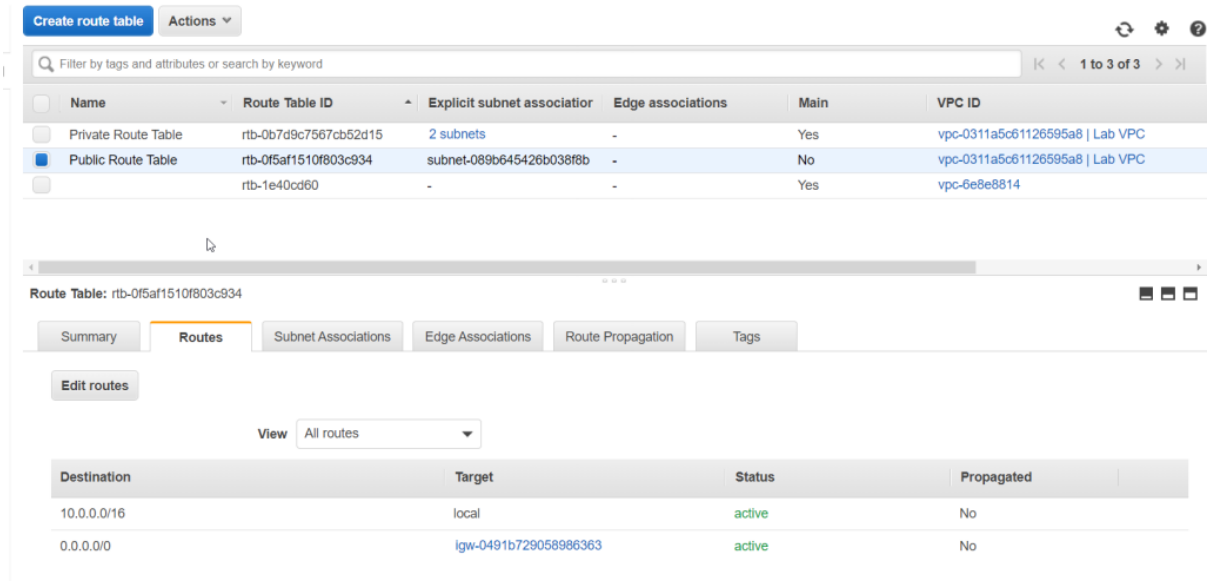


Added **Private Subnet 1** and **Private Subnet 2**. into this private routing table

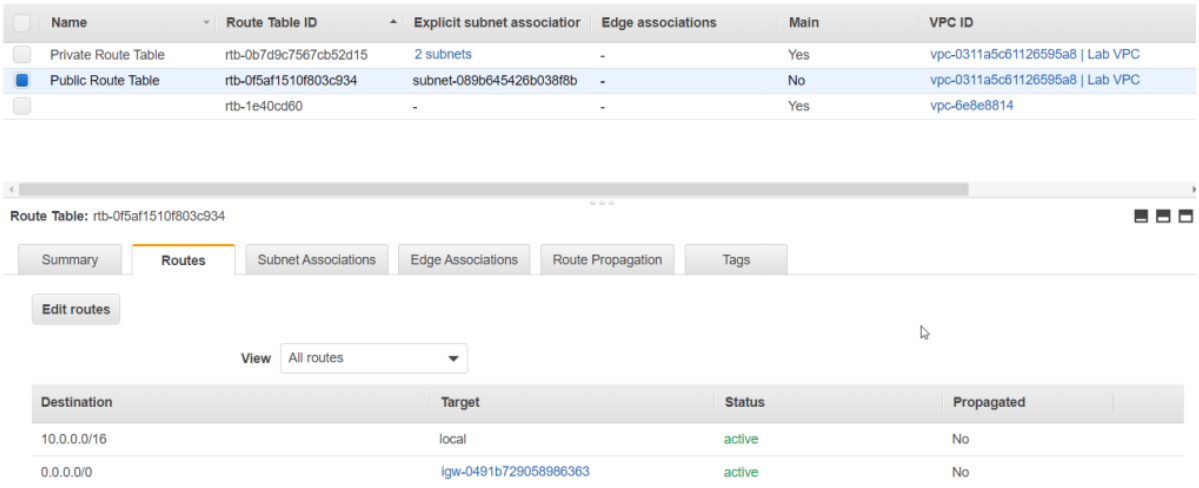
Below are the steps to configure public routing table :



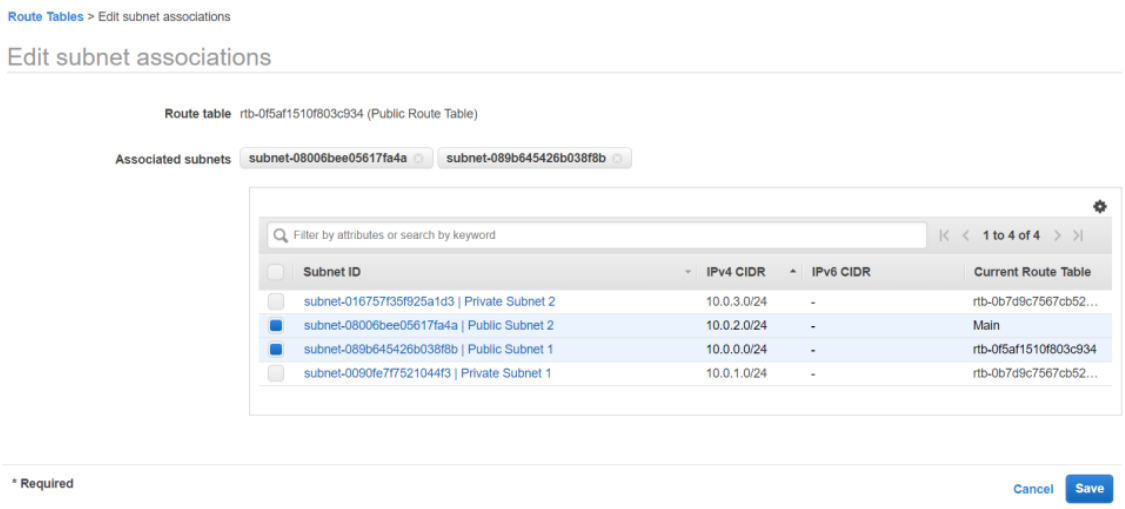
Select the route table with Main = No and VPC = Lab VPC



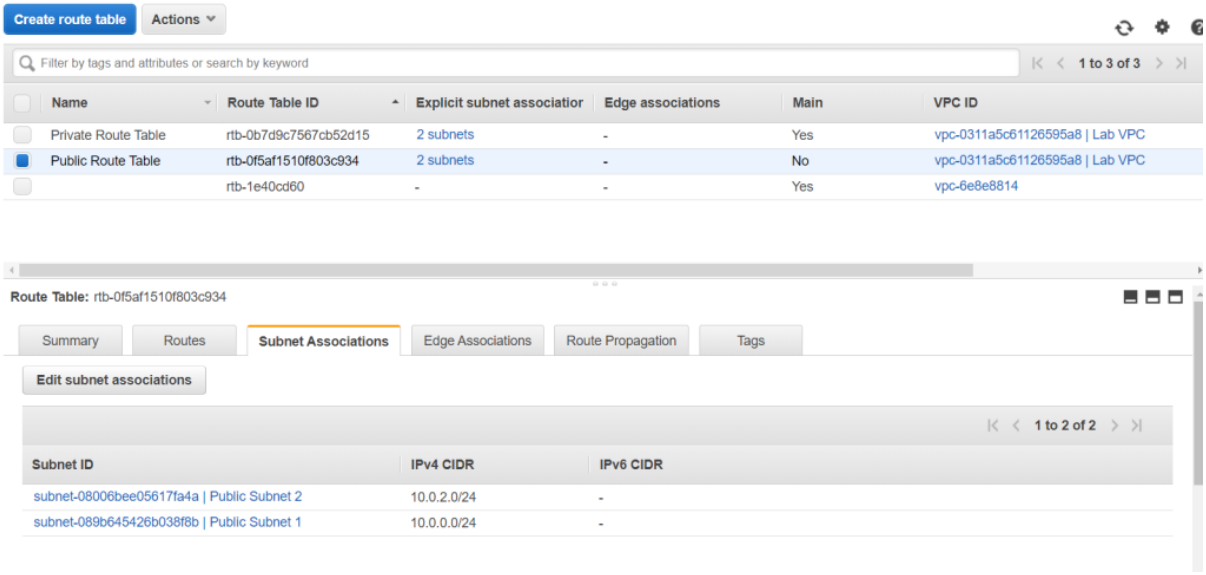
Named it as Public Route Table



Note that **Destination 0.0.0.0/0** is set to **Target igw-xxxxxxxx**, which is the Internet Gateway. This means that internet-bound traffic will be sent straight to the internet via the Internet Gateway.



Associate Public subnets to this Public route table



Task 3: Create a VPC Security Group

In this task, you will create a VPC security group, which acts as a virtual firewall. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

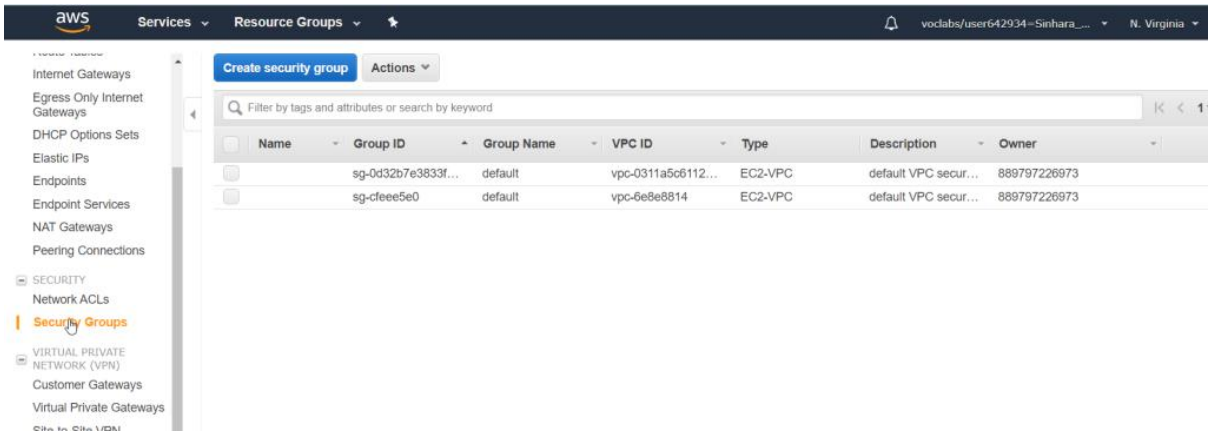


Figure 6.23

left navigation pane, click **Security Groups**.

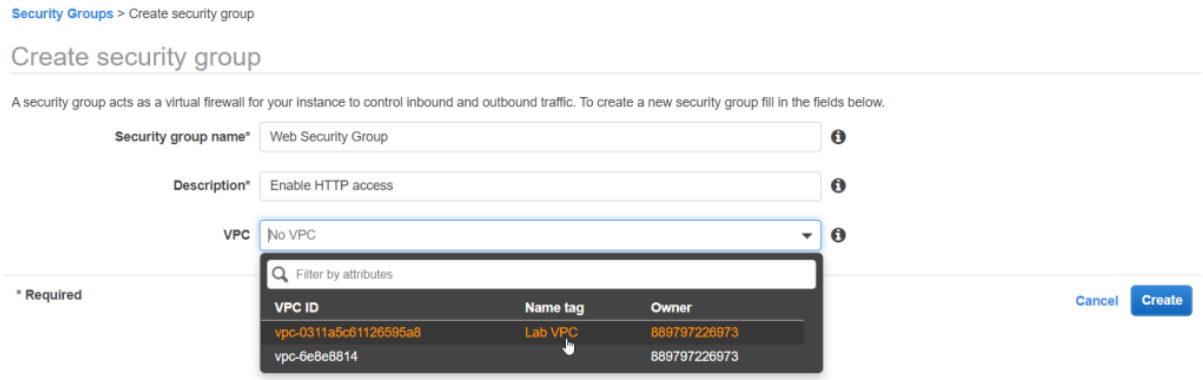


Figure 6.24

Create security group with Security group name: Web Security Group,Description: Enable HTTP access,VPC: Lab VPC

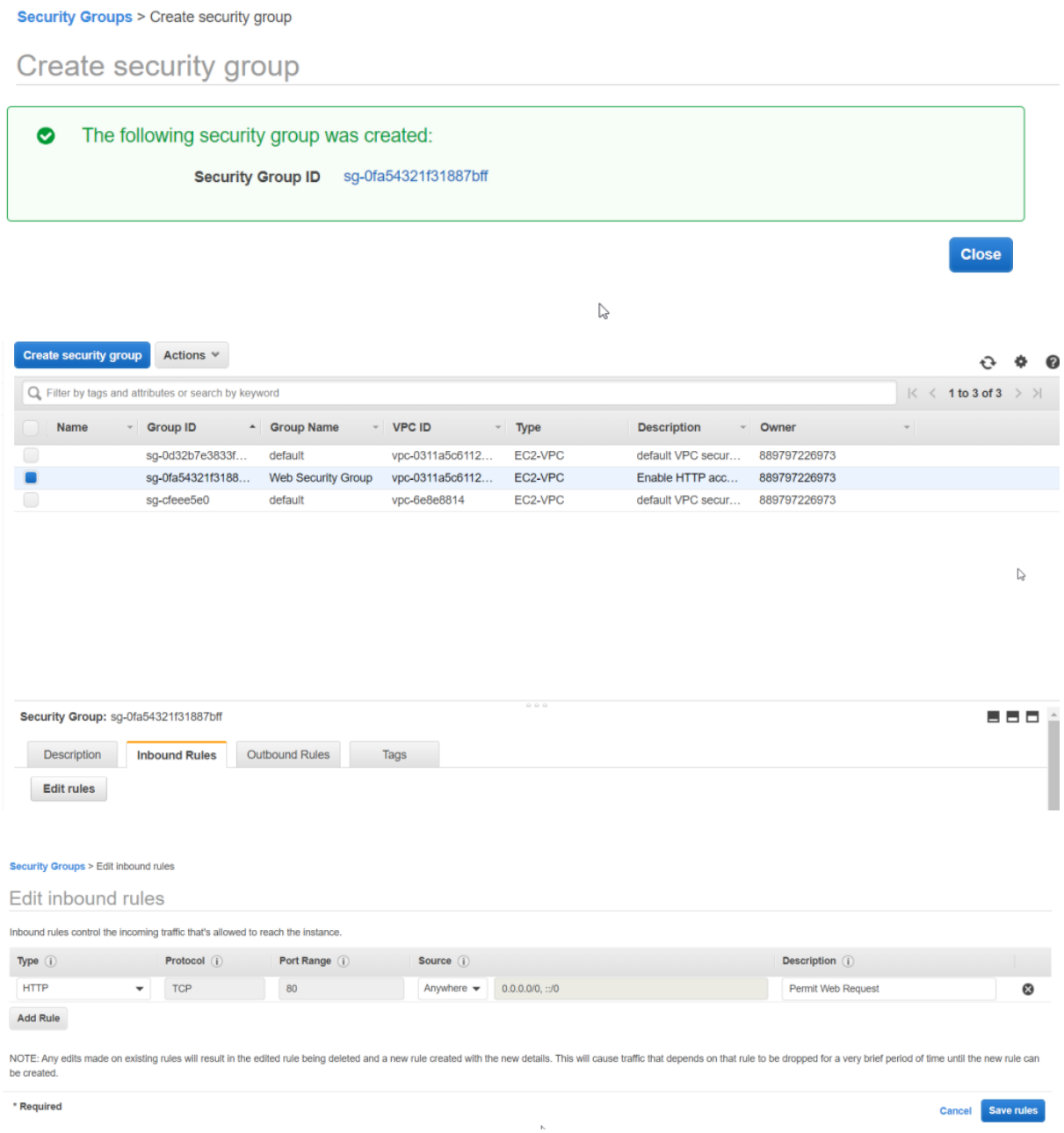

Security Groups > Create security group
Create security group
The following security group was created:
Security Group ID sg-0fa54321f31887bff
Close
Create security group
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Group ID
Group Name
VPC ID
Type
Description
Owner
sg-0d32b7e3833f...
default
vpc-0311a5c6112...
EC2-VPC
default VPC secur...
889797226973
sg-0fa54321f3188...
Web Security Group
vpc-0311a5c6112...
EC2-VPC
Enable HTTP acc...
889797226973
sg-cfeee5e0
default
vpc-6e8e8814
EC2-VPC
default VPC secur...
889797226973
Security Group: sg-0fa54321f31887bff
Description
Inbound Rules
Outbound Rules
Tags
Edit rules
Security Groups > Edit inbound rules
Edit inbound rules
Inbound rules control the incoming traffic that's allowed to reach the instance.
Type
Protocol
Port Range
Source
Description
HTTP
TCP
80
Anywhere
0.0.0.0/0, ::/0
Permit Web Request
Add Rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.
* Required
Cancel
Save rules

Figure 6.25

Allow HTTP request inbound direction from anywhere

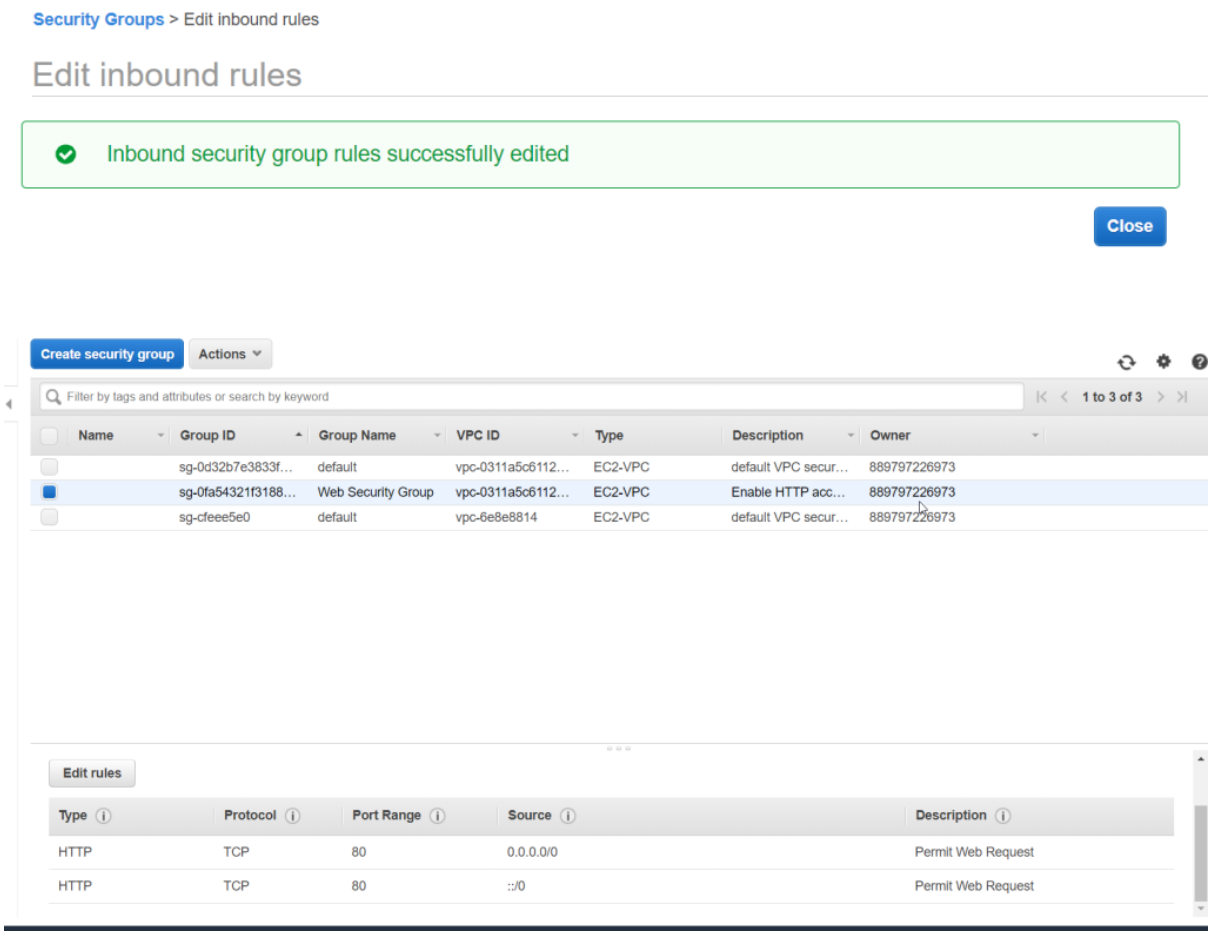


Figure 6.26

Task 4: Launch a Web Server Instance

In this task, you will launch an Amazon EC2 instance into the new VPC. You will configure the instance to act as a web server.

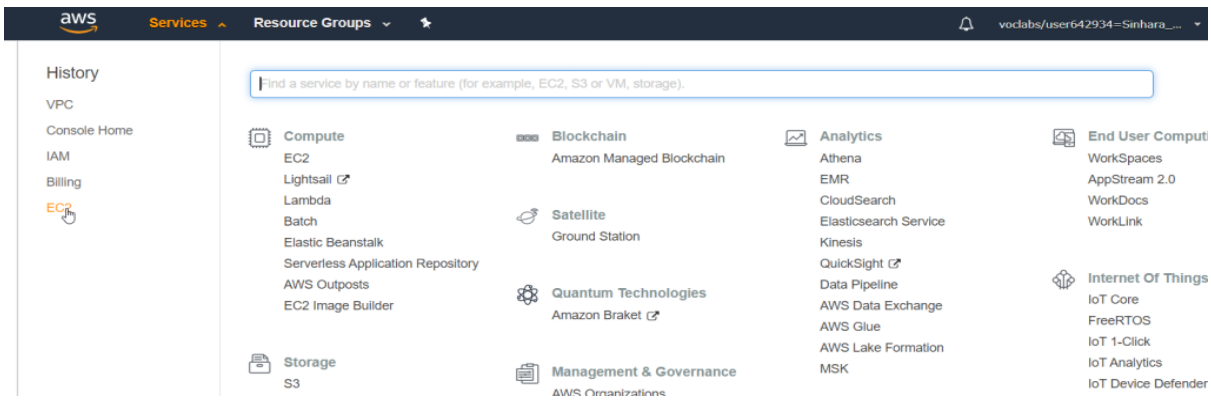


Figure 6.27

Invoking EC2 services

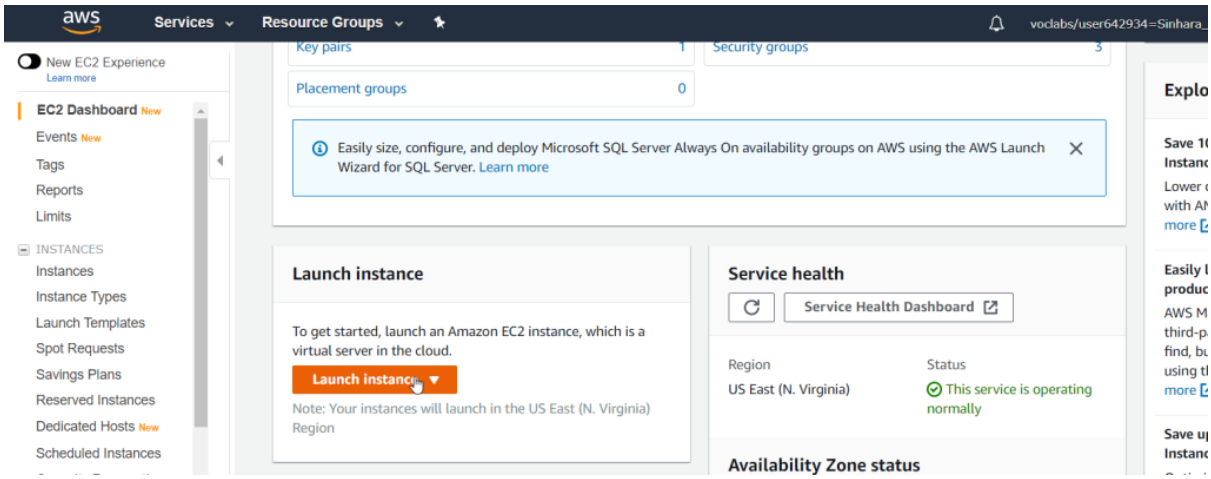


Figure 6.28

Invoking EC2 services

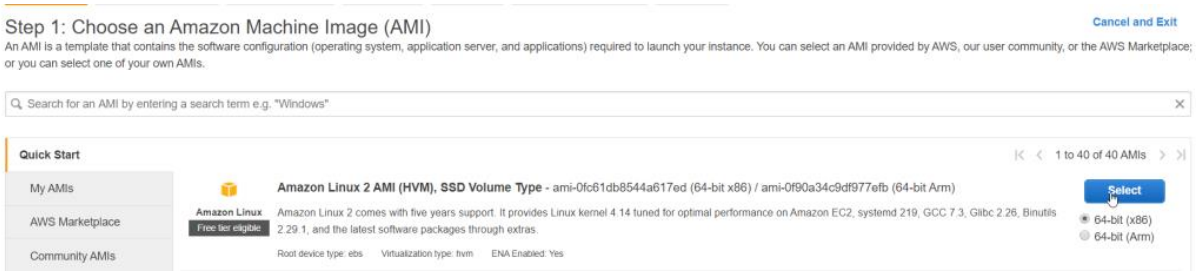


Figure 6.29

Select “**Amazon Linux 2**” instance

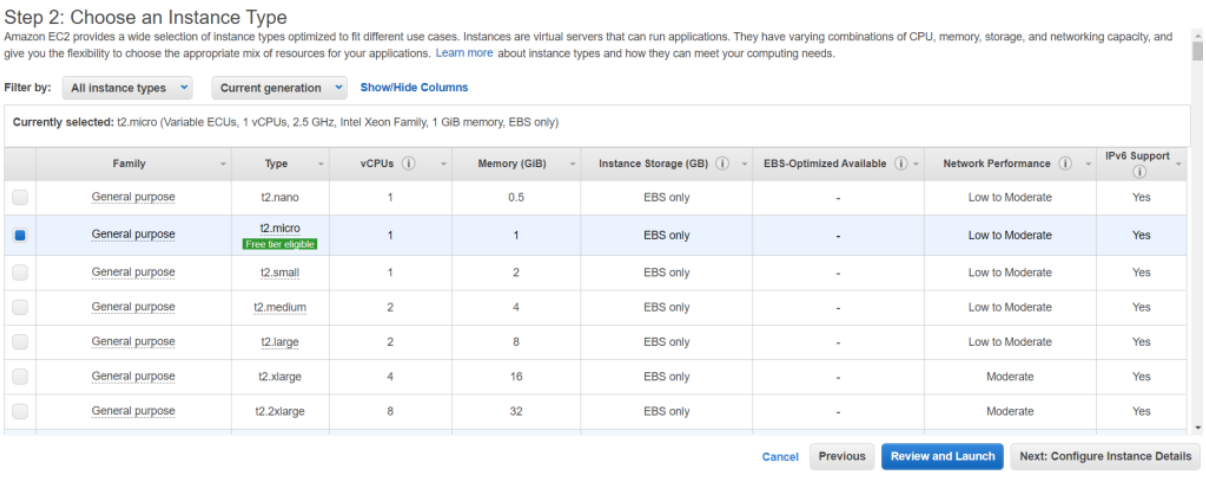


Figure 6.30

Select “t2.micro” as instance profile

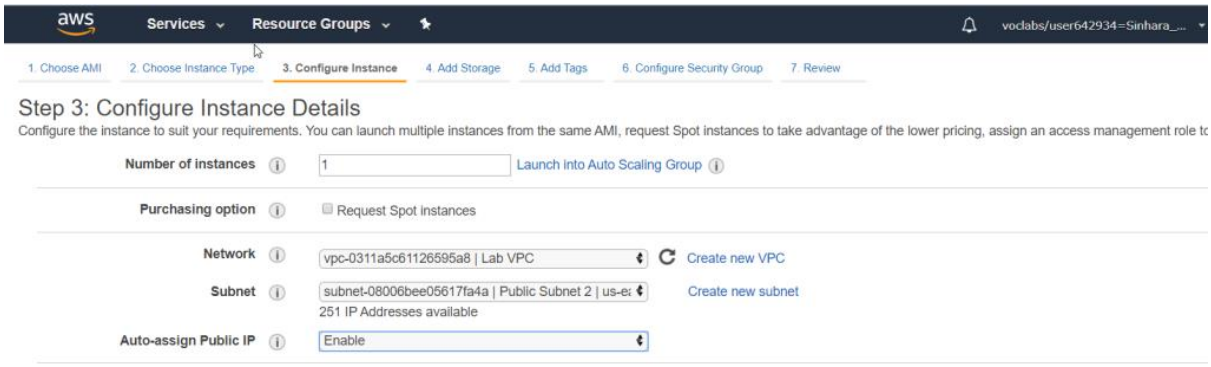


Figure 6.31

Configure Network: Lab VPC, Subnet: Public Subnet 2 (not Private!),Auto-assign Public IP: Enable

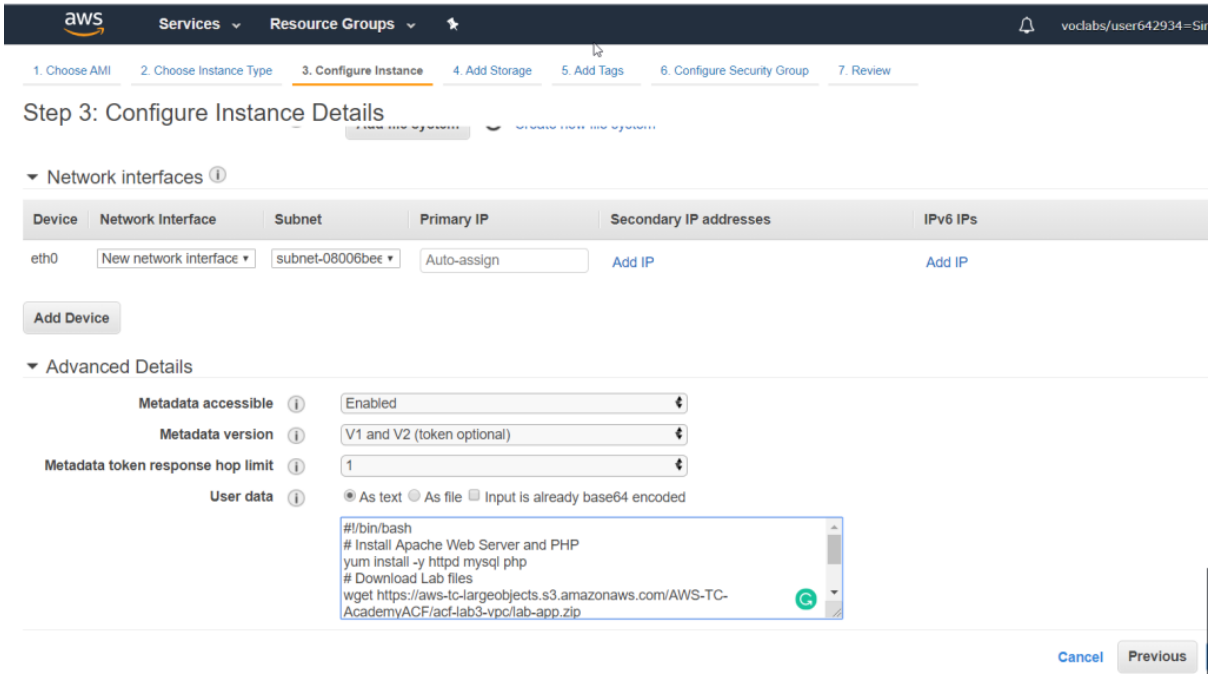


Figure 6.32

Copy and paste this code into the User data box:

!/bin/bash

Install Apache Web Server and PHP

yum install -y httpd mysql php

Download Lab files

wget https://aws-tc-largeobjects.s3.amazonaws.com/AWS-TC-AcademyACF/acf-lab3-vpc/lab-app.zip

unzip lab-app.zip -d /var/www/html/

Turn on web server

chkconfig httpd on

service httpd start

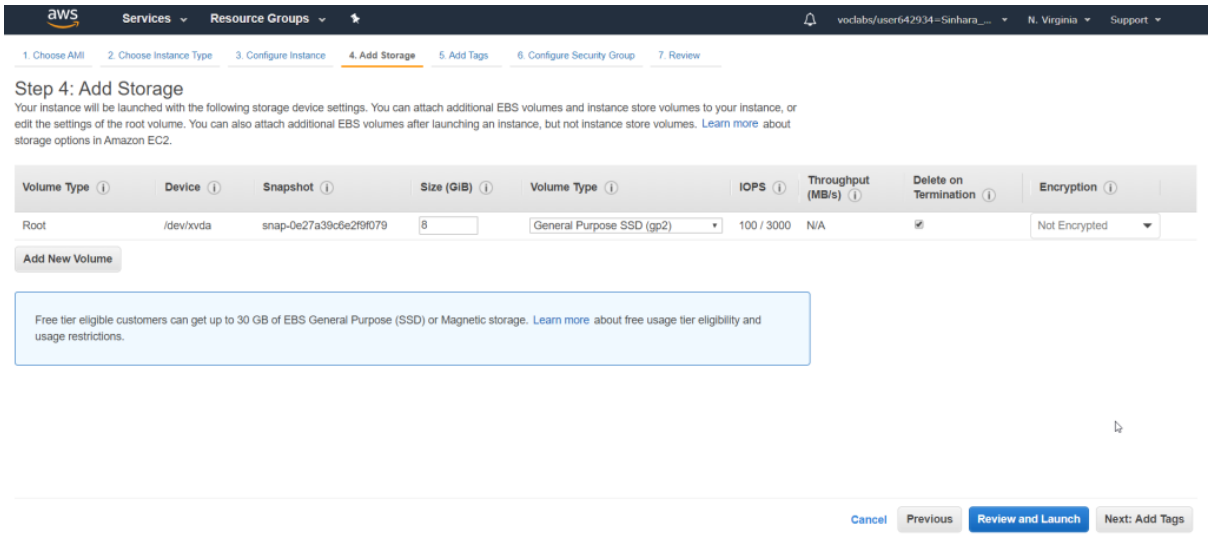


Figure 6.33

Leave default settings

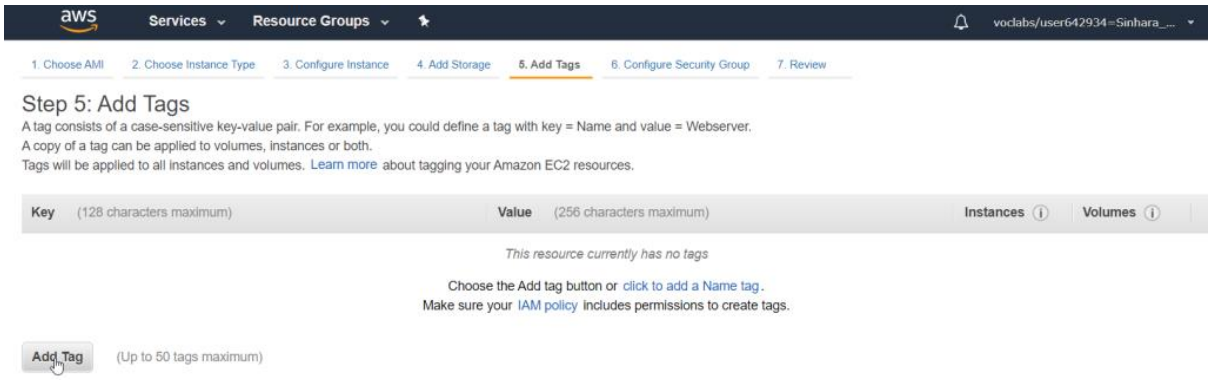


Figure 6.34

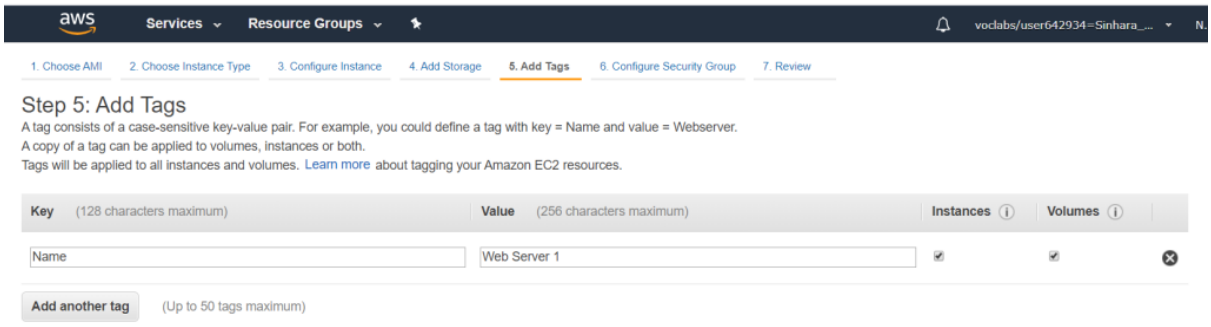


Figure 6.35

Click **Add Tag** then configure: **Key:** Name, **Value:** Web Server 1

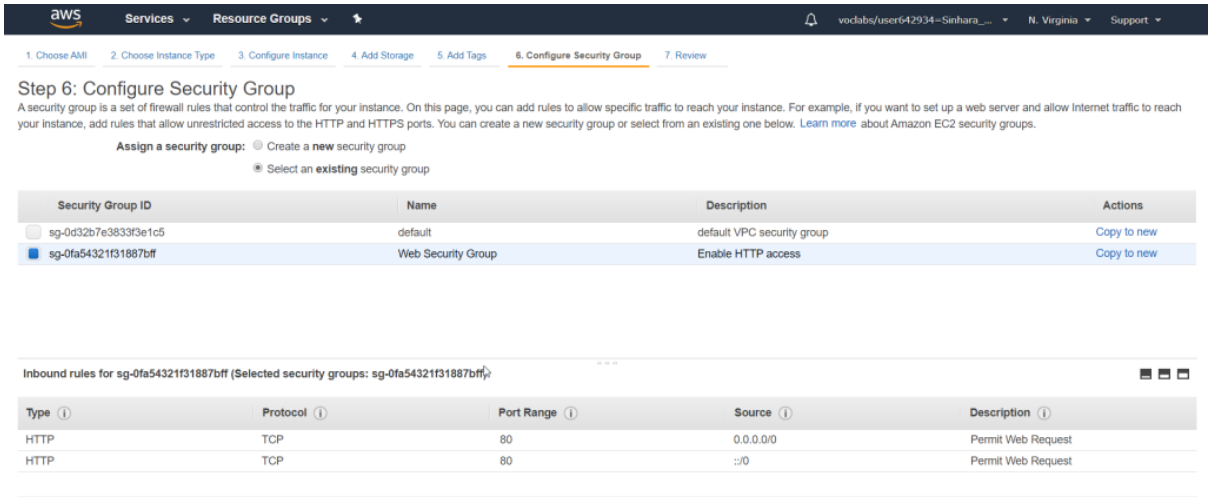
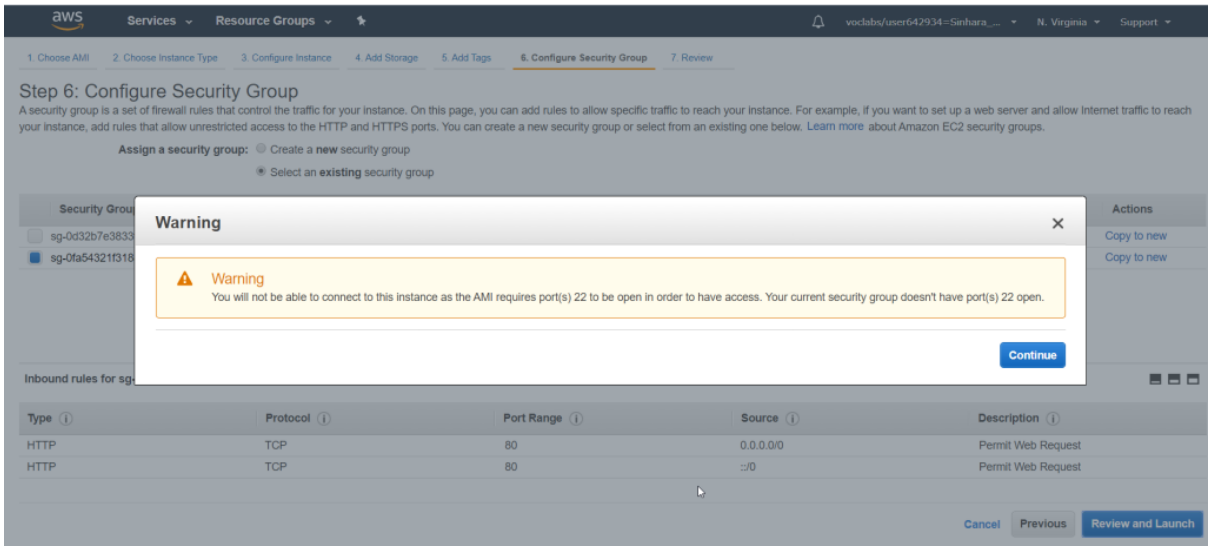
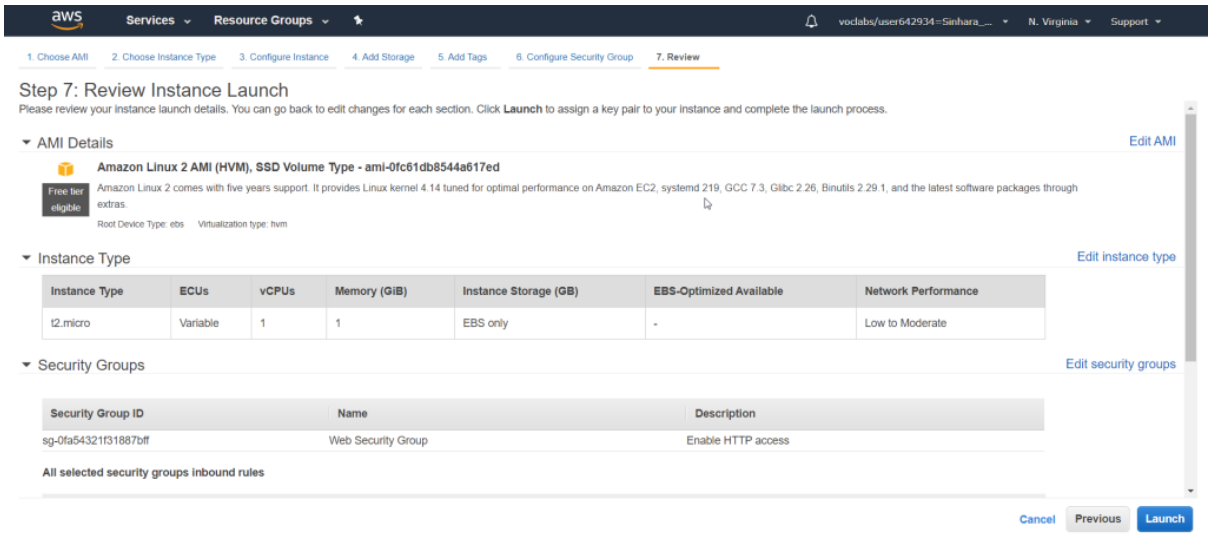


Figure 6.36

Select **Select an existing security group**, Select **Web Security Group**.



When prompted with a *warning* that you will not be able to connect to the instance through port 22, click **Continue**



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

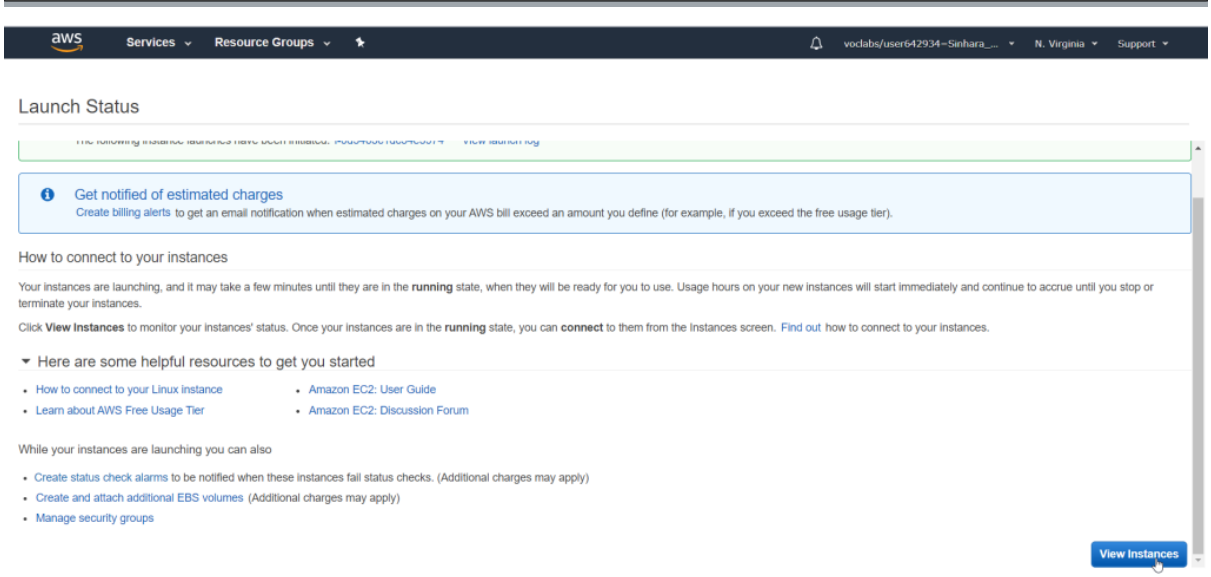
Choose an existing key pair

Select a key pair

vockey

I acknowledge that I have access to the selected private key file (vockey.pem), and that without this file, I won't be able to log into my instance.

Cancel | Launch Instances



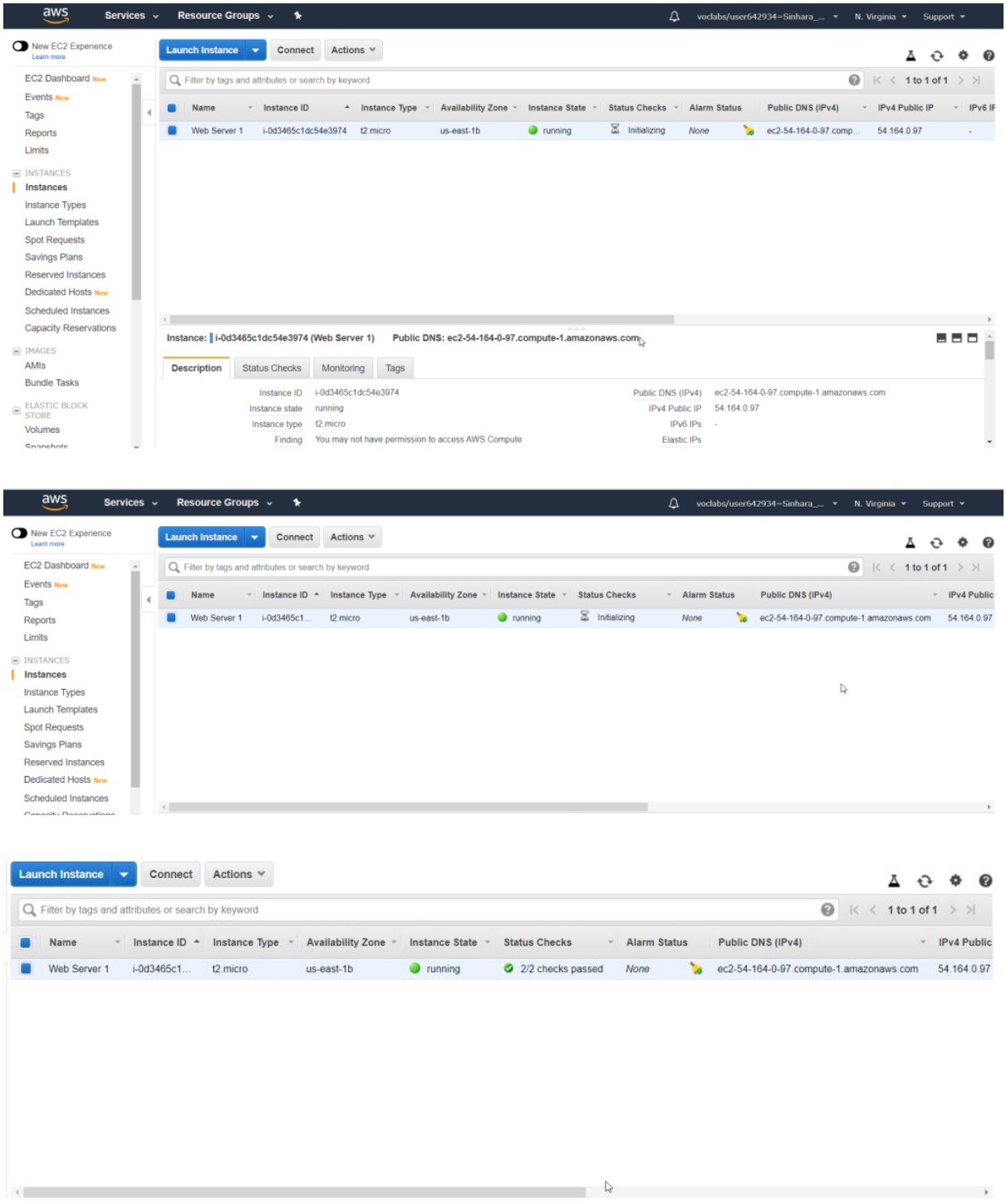


Figure 6.42

Copy public DNS : ec2-54-164-0-97.compute-1.amazonaws.com

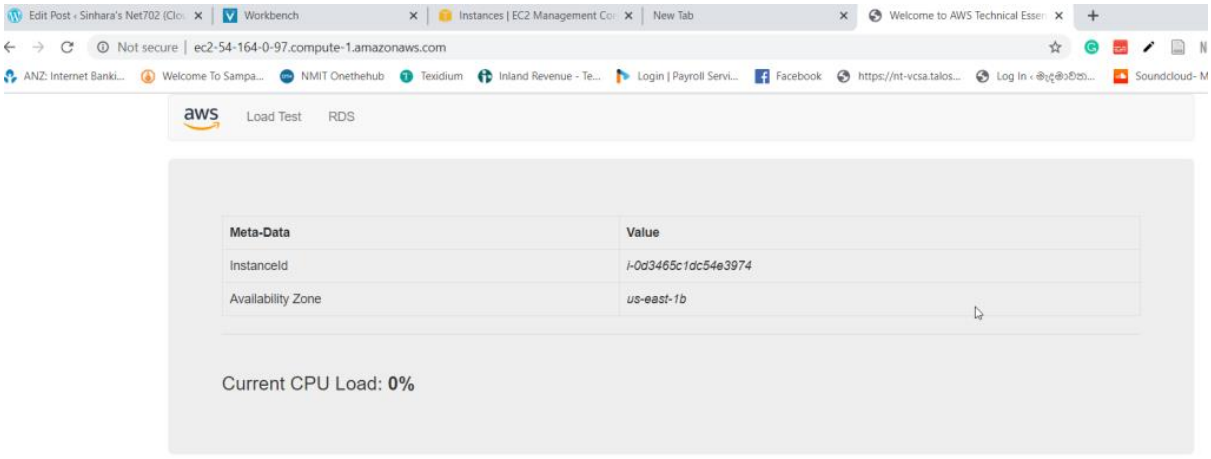


Figure 6.43

Open a new web browser tab, paste the **Public DNS** value and press Enter.

You should see a web page displaying the AWS logo and instance meta-data values.

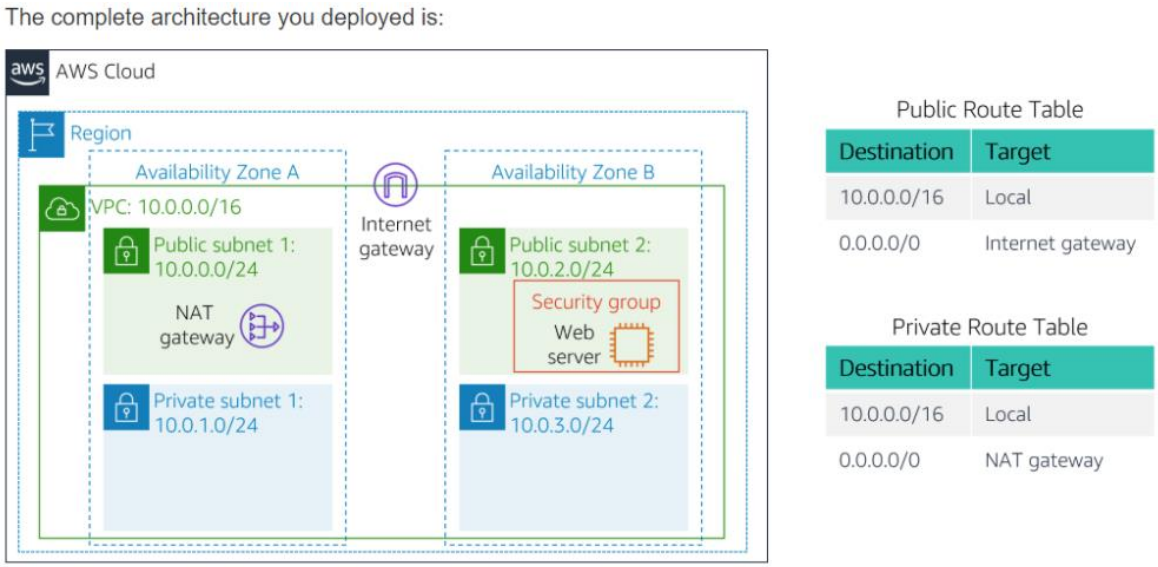


Figure 6.44

Result:

The experiment was successfully executed on AWS free tier in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-7

Date:

<u>Aim:</u> Introduction to Amazon EC2

Accessing the AWS Management Console

1. At the top of these instructions, choose Start Lab to launch your lab. A Start Lab panel opens displaying the lab status.
2. Wait until you see the message "**Lab status: ready**", then choose the **X** to close the Start Lab panel.
3. At the top of these instructions, choose AWS This will open the AWS Management Console in a new browser tab. The system will automatically log you in.
   Tip: If a new browser tab does not open, there will typically be a banner or icon at the top of your browser indicating that your browser is preventing the site from opening pop-up windows. Choose on the banner or icon and choose "Allow pop ups."
4. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you will be able to see both browser tabs at the same time, to make it easier to follow the lab steps.

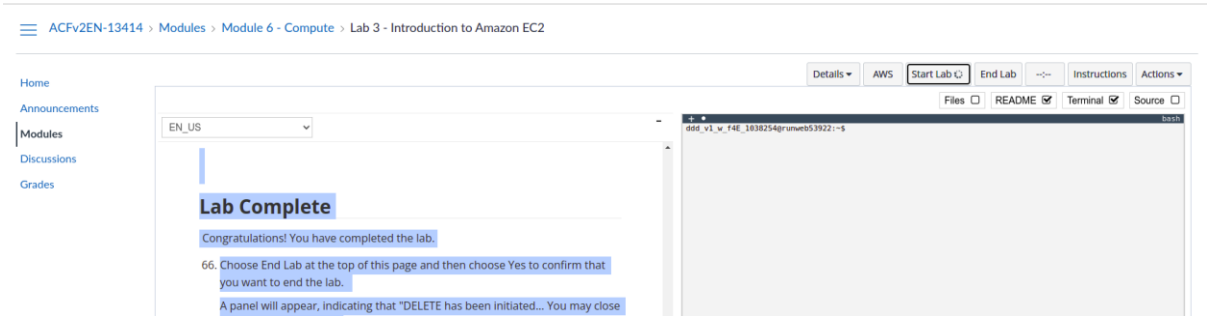


Figure 7.1

Task 1: Launch Your Amazon EC2 Instance

In this task, you will launch an Amazon EC2 instance with *termination protection*. Termination protection prevents you from accidentally terminating an EC2 instance. You will deploy your instance with a User Data script that will allow you to deploy a simple web server.

5. In the **AWS Management Console** on the **Services** menu, choose **EC2**. **Note**: Verify that your EC2 console is currently managing resources in the **N. Virginia** (us-east-1) region. You can verify this by looking at the drop down menu at the top of the screen, to the left of your username. If it does not already indicate N. Virginia, choose the N. Virginia region from the region menu before proceeding to the next step.
6. Choose Launch instance , then select Launch Instance

Step 1: Choose an Amazon Machine Image (AMI)

An **Amazon Machine Image (AMI)** provides the information required to launch an instance, which is a virtual server in the cloud. An AMI includes:

- A template for the root volume for the instance (for example, an operating system or an application server with applications)
- Launch permissions that control which AWS accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when it is launched

The **Quick Start** list contains the most commonly-used AMIs. You can also create your own AMI or select an AMI from the AWS Marketplace, an online store where you can sell or buy software that runs on AWS.

7. Choose Select next to **Amazon Linux 2 AMI** (at the top of the list).

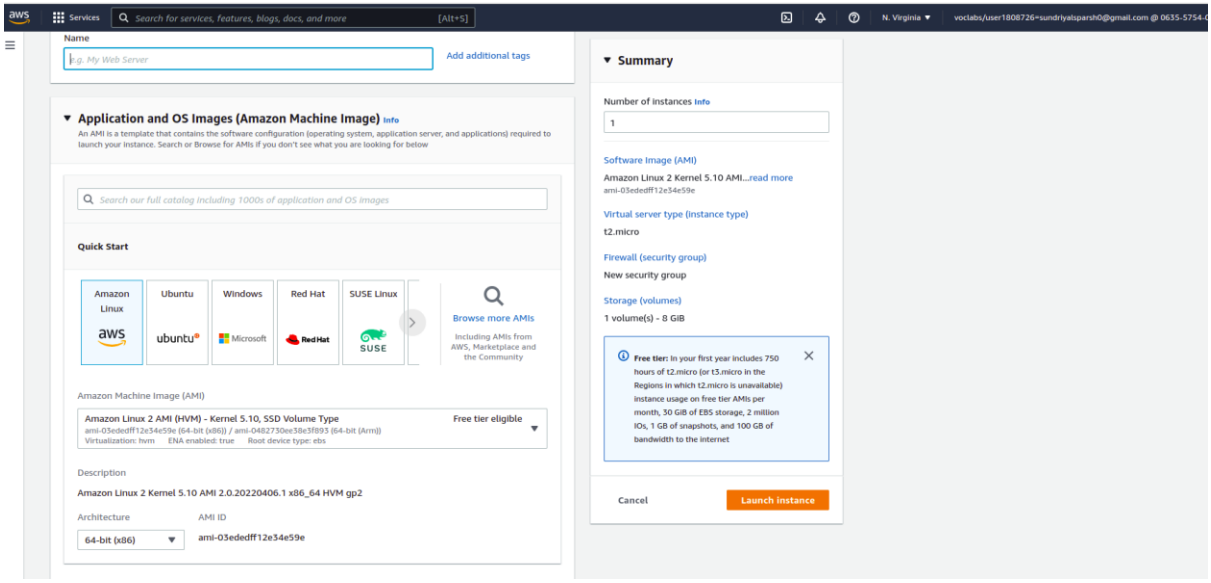


Figure 7.2

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more *instance sizes*, allowing you to scale your resources to the requirements of your target workload.

You will use a **t2.micro** instance which should be selected by default. This instance type has 1 virtual CPU and 1 GiB of memory. **NOTE**: You may be restricted from using other instance types in this lab.

8. Choose Next: Configure Instance Details

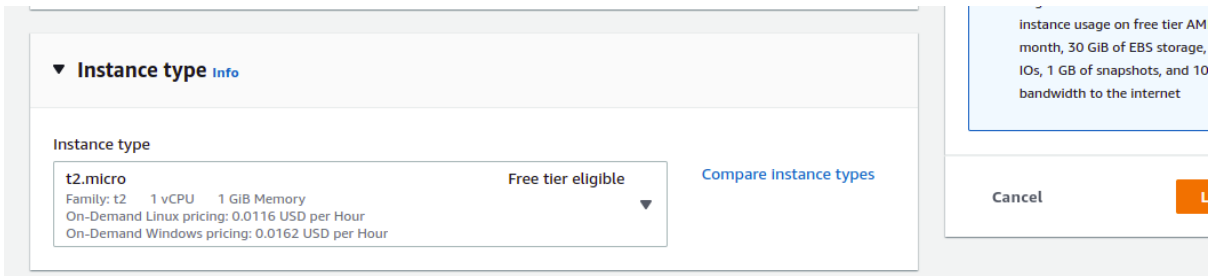


Figure 7.3

Step 3: Configure Instance Details

This page is used to configure the instance to suit your requirements. This includes networking and monitoring settings.

The **Network** indicates which Virtual Private Cloud (VPC) you wish to launch the instance into. You can have multiple networks, such as different ones for development, testing and production.

9. For **Network**, select **Lab VPC**.
   The Lab VPC was created using an AWS CloudFormation template during the setup process of your lab. This VPC includes two public subnets in two different Availability Zones.
10. For **Enable termination protection**, select **Protect against accidental termination**.

When an Amazon EC2 instance is no longer required, it can be *terminated*, which means that the instance is stopped and its resources are released. A terminated instance cannot be started again. If you want to prevent the instance from being accidentally terminated, you can enable *termination protection* for the instance, which prevents it from being terminated.

11. Scroll down, then expand **Advanced Details**.

A field for **User data** will appear.

When you launch an instance, you can pass *user data* to the instance that can be used to perform common automated configuration tasks and even run scripts after the instance starts.

Your instance is running Amazon Linux, so you will provide a *shell script* that will run when the instance starts.

12. Copy the following commands and paste them into the **User data** field:
13. #!/bin/bash

```
yum -y install httpd
systemctl enable httpd
systemctl start httpd
```

```
echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
```

14. The script will:
    - Install an Apache web server (httpd)
    - Configure the web server to automatically start on boot
    - Activate the Web server
    - Create a simple web page
13. Choose Next: Add Storage

Step 4: Add Storage

Amazon EC2 stores data on a network-attached virtual disk called *Elastic Block Store*.

You will launch the Amazon EC2 instance using a default 8 GiB disk volume. This will be your root volume (also known as a 'boot' volume).

14. Choose Next: Add Tags

Step 5: Add Tags

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you have assigned to it. Each tag consists of a Key and a Value, both of which you define.

15. Choose Add Tag then configure:
    - **Key:** Name
    - **Value:** Web Server
16. Choose Next: Configure Security Group

Step 6: Configure Security Group

A *security group* acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add *rules* to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.

17. On **Step 6: Configure Security Group**, configure:
    - **Security group name:** Web Server security group
    - **Description:** Security group for my web server
18. In this lab, you will not log into your instance using SSH. Removing SSH access will improve the security of the instance.
19. Delete the existing SSH rule.
20. Choose Review and Launch

Step 7: Review Instance Launch

The Review page displays the configuration for the instance you are about to launch.

20. Choose Launch

A **Select an existing key pair or create a new key pair** window will appear.

Amazon EC2 uses public–key cryptography to encrypt and decrypt login information. To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.

In this lab you will not log into your instance, so you do not require a key pair.

21. Choose the **Choose an existing key pair** drop-down and select *Proceed without a key pair*.
22. Select **I acknowledge that ....**

23. Choose Launch Instances
    Your instance will now be launched.
24. Choose View Instances
    The instance will appear in a *pending* state, which means it is being launched. It will then change to *running*, which indicates that the instance has started booting. There will be a short time before you can access the instance.
    The instance receives a *public DNS name* that you can use to contact the instance from the Internet.
    Your **Web Server** should be selected. The **Description** tab displays detailed information about your instance.
    To view more information in the Description tab, drag the window divider upwards. Review the information displayed in the **Details** tab. It includes information about the instance type, security settings and network settings.
25. Wait for your instance to display the following:

- **Instance State:** running
- **Status Checks:** 2/2 checks passed

Congratulations! You have successfully launched your first Amazon EC2 instance.

Task 2: Monitor Your Instance

Monitoring is an important part of maintaining the reliability, availability, and performance of your Amazon Elastic Compute Cloud (Amazon EC2) instances and your AWS solutions.

26. Choose the **Status Checks** tab.
    With instance status monitoring, you can quickly determine whether Amazon EC2 has detected any problems that might prevent your instances from running applications. Amazon EC2 performs automated checks on every running EC2 instance to identify hardware and software issues.
    Notice that both the **System reachability** and **Instance reachability** checks have passed.

27. Choose the **Monitoring** tab.
    This tab displays Amazon CloudWatch metrics for your instance. Currently, there are not many metrics to display because the instance was recently launched. You can choose on a graph to see an expanded view.
    Amazon EC2 sends metrics to Amazon CloudWatch for your EC2 instances. Basic (five-minute) monitoring is enabled by default. You can enable detailed (one-minute) monitoring.
28. In the Actions menu, select **Monitor and troubleshoot Get system log**. The System Log displays the console output of the instance, which is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started. If you do not see a system log, wait a few minutes and then try again.
29. Scroll through the output and note that the HTTP package was installed from the **user data** that you added when you created the instance.

30. Choose **Cancel**.
31. In the Actions menu, select **Monitor and troubleshoot Get instance screenshot**. This shows you what your Amazon EC2 instance console would look like if a screen were attached to it.

    If you are unable to reach your instance via SSH or RDP, you can capture a screenshot of your instance and view it as an image. This provides visibility as to the status of the instance, and allows for quicker troubleshooting.
32. Choose **Cancel**.

    Congratulations! You have explored several ways to monitor your instance.

Task 3: Update Your Security Group and Access the Web Server

When you launched the EC2 instance, you provided a script that installed a web server and created a simple web page. In this task, you will access content from the web server.

33. Choose the **Details** tab.

34. Copy the **IPv4 Public IP** of your instance to your clipboard.
35. Open a new tab in your web browser, paste the IP address you just copied, then press **Enter**.

    Question: Are you able to access your web server? Why not?
    You are **not** currently able to access your web server because the *security group* is not permitting inbound traffic on port 80, which is used for HTTP web requests. This is a demonstration of using a security group as a firewall to restrict the network traffic that is allowed in and out of an instance.
    To correct this, you will now update the security group to permit web traffic on port 80.
36. Keep the browser tab open, but return to the **EC2 Management Console** tab.
37. In the left navigation pane, choose **Security Groups**.
38. Select **Web Server security group**.
39. Choose the **Inbound rules** tab.
    The security group currently has no rules.
40. Choose Edit inboud rules then configure:
    - **Type:** *HTTP*
    - **Source:** *Anywhere-IPv4*
    - Choose Save rules
41. Return to the web server tab that you previously opened and refresh the page. You should see the message *Hello From Your Web Server!* **Congratulations!** You have successfully modified your security group to permit HTTP traffic into your Amazon EC2 Instance.

Task 4: Resize Your Instance: Instance Type and EBS Volume

As your needs change, you might find that your instance is over-utilized (too small) or under-utilized (too large). If so, you can change the *instance type*. For example, if a *t2.micro* instance is too small for its workload, you can change it to an *m5.medium* instance. Similarly, you can change the size of a disk.

Stop Your Instance

Before you can resize an instance, you must *stop* it.

When you stop an instance, it is shut down. There is no charge for a stopped EC2 instance, but the storage charge for attached Amazon EBS volumes remains.

42. On the **EC2 Management Console**, in the left navigation pane, choose **Instances**. **Web Server** should already be selected.
43. In the Instance State menu, select **Stop instance**.
44. Choose Stop
    Your instance will perform a normal shutdown and then will stop running.
45. Wait for the **Instance State** to display: stopped

Change The Instance Type

46. In the Actions menu, select **Instance Settings Change Instance Type**, then configure:
    - **Instance Type:** *t2.small*
    - Choose Apply
47. When the instance is started again it will be a *t2.small*, which has twice as much memory as a *t2.micro* instance. **NOTE**: You may be restricted from using other instance types in this lab.

Resize the EBS Volume

47. In the left navigation menu, choose **Volumes**.
48. In the Actions menu, select **Modify Volume**.
    The disk volume currently has a size of 8 GiB. You will now increase the size of this disk.
49. Change the size to: 10 **NOTE**: You may be restricted from creating large Amazon EBS volumes in this lab.
50. Choose Modify
51. Choose Yes to confirm and increase the size of the volume.
52. Choose Close

Start the Resized Instance

You will now start the instance again, which will now have more memory and more disk space.

53. In left navigation pane, choose **Instances**.
54. In the Instance State menu, select **Start instance**.
55. Choose Start

Congratulations! You have successfully resized your Amazon EC2 Instance. In this task you changed your instance type from *t2.micro* to *t2.small*. You also modified your root disk volume from 8 GiB to 10 GiB.

Task 5: Explore EC2 Limits

Amazon EC2 provides different resources that you can use. These resources include images, instances, volumes, and snapshots. When you create an AWS account, there are default limits on these resources on a per-region basis.

56. In the left navigation pane, choose **Limits**.
57. From the drop down list, choose **Running instances**.
    Note that there is a limit on the number of instances that you can launch in this region. When launching an instance, the request must not cause your usage to exceed the current instance limit in that region.
    You can request an increase for many of these limits.

Task 6: Test Termination Protection

You can delete your instance when you no longer need it. This is referred to as *terminating* your instance. You cannot connect to or restart an instance after it has been terminated.

In this task, you will learn how to use *termination protection*.

58. In left navigation pane, choose **Instances**.
59. In the Instance state menu, select **Terminate instance**.
60. Then choose Terminate
    Note that there is a message that says: *Failed to terminate the instance i-1234567xxx. The instance 'i-1234567xxx' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.*
    This is a safeguard to prevent the accidental termination of an instance. If you really want to terminate the instance, you will need to disable the termination protection.

61. In the Actions menu, select **Instance settings Change termination protection**.
62. Remove the check next to **Enable**.
63. Choose Save

    You can now terminate the instance.
64. In the Instance state menu, select **Terminate instance**.
65. Choose Terminate

    Congratulations! You have successfully tested termination protection and terminated your instance.

Lab Complete

Congratulations! You have completed the lab.

66. Choose End Lab at the top of this page and then choose Yes to confirm that you want to end the lab.

    A panel will appear, indicating that "DELETE has been initiated... You may close this message box now."
67. Choose the **X** in the top right corner to close the panel.

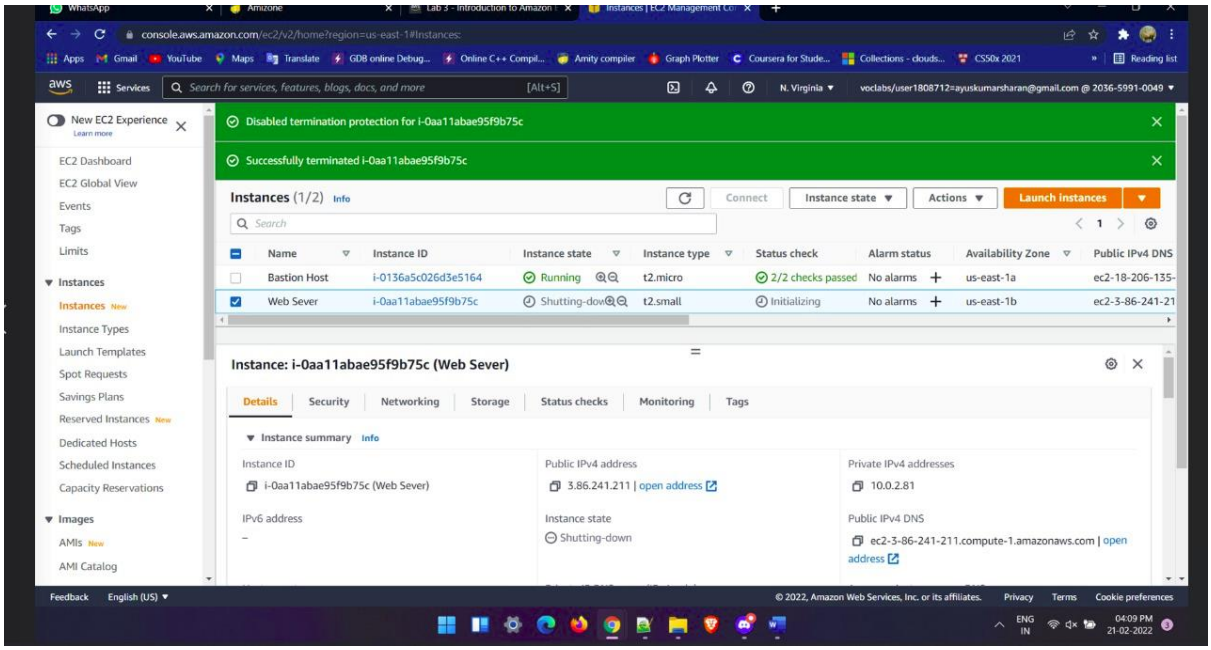


Figure 7.4

Result:

The experiment was successfully executed on AWS free tier in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-8

Date:

<u>Aim:</u> Build a Database and interact with it using an Application.

First of all, you have to create users and configure a *security group which* works as a virtual firewall for your application to regulate inbound and outbound traffic with following details

- Name tag: DB-Security-Group
- Group: DB-Security-Group
- Description: DB Instance Security Group
- VPC: MyLab VPC

and click on create button. After this select one group and modify its inbound rule. change the values of a text field.

- Type: MySQL
- Protocol: TCP(6)
- Source: Web-Security-Group

Amazon Relational Database Service (Amazon RDS) help users to create and functioning of a relational database in the cloud. It gives resizable capacity at low cost.In the services, menu clicks on Relational Database Service and create subnet group. Click on **Create DB Subnet Group** and fill the following figures

- Name : db-subnet-group
- description: DB Instance Subnet Group
- VPC ID: My Lab VPC
- Availability Zone: First AZ
- subnet : 10.0.4.0/24

and now create a new subnet in the second Availability Zone

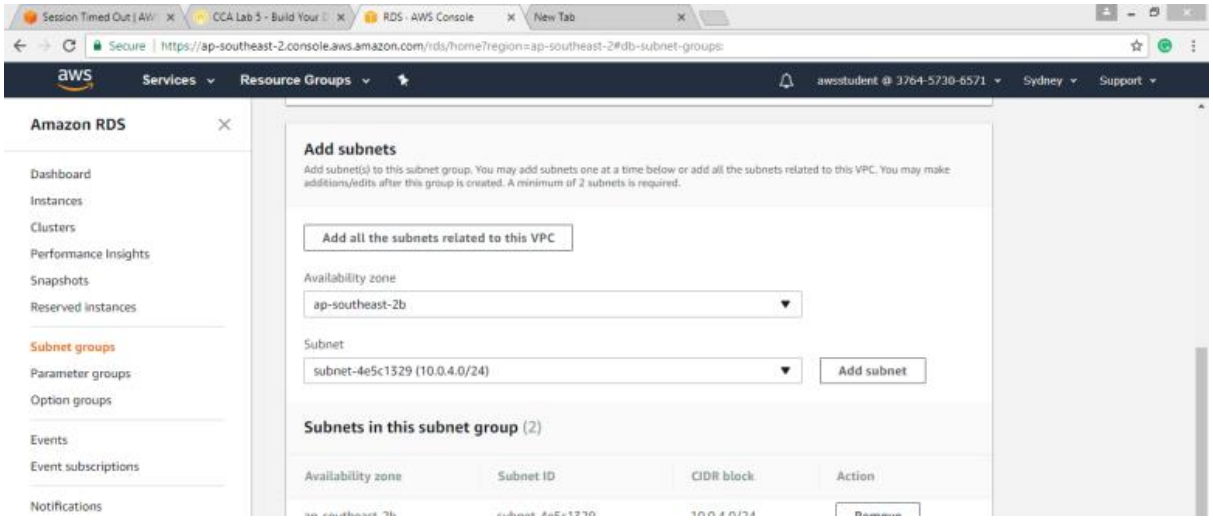


Figure 8.1

On the left, click on an instance, and click on Launch after that select MySQL.

For using Use Case select Production-MYSQL and then click on Next.

A new page will be open where specific DB details will be asked:

- DB Instance class : db.t2.micro (first select)
- DB instance identifier:lab-db
- Master username: master
- Master password: lab-password
- Confirm Password: lab-Password

click on next, configure advanced settings will be asked.

- VPC: My Lab VPC
- Subnet group: db-subnet-group
- VPC Security groups: select one in existing
- select VPC security groups: DB-Security-Group and remove the default
- database name: lab
- Backup retention period :0
- Enhanced monitoring: Disable

These setting will disable all backup services. Now you can launch the instances of the class,

Open EC2 instance again, now you will see Web server 1. Copy its IP4 address and paste in a new tab of the web browser. Click RDS link on screen it makes a connection between application and database, Application can be seen on the screen. Configure the following details.

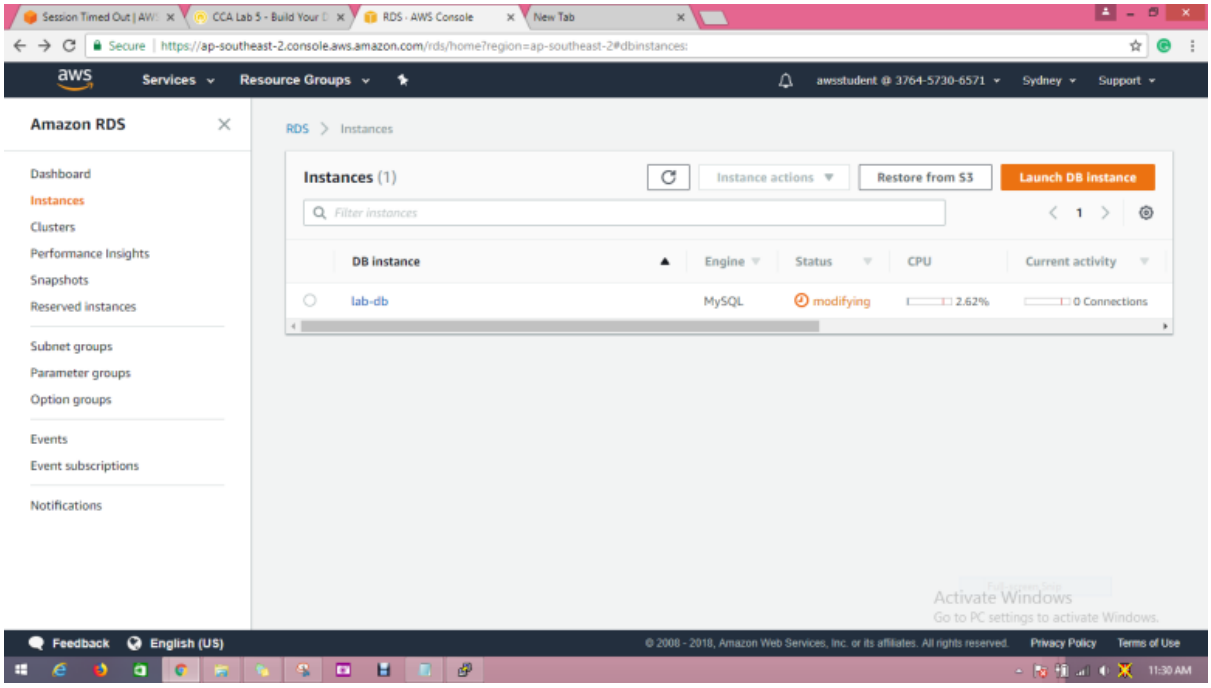


Figure 8.2

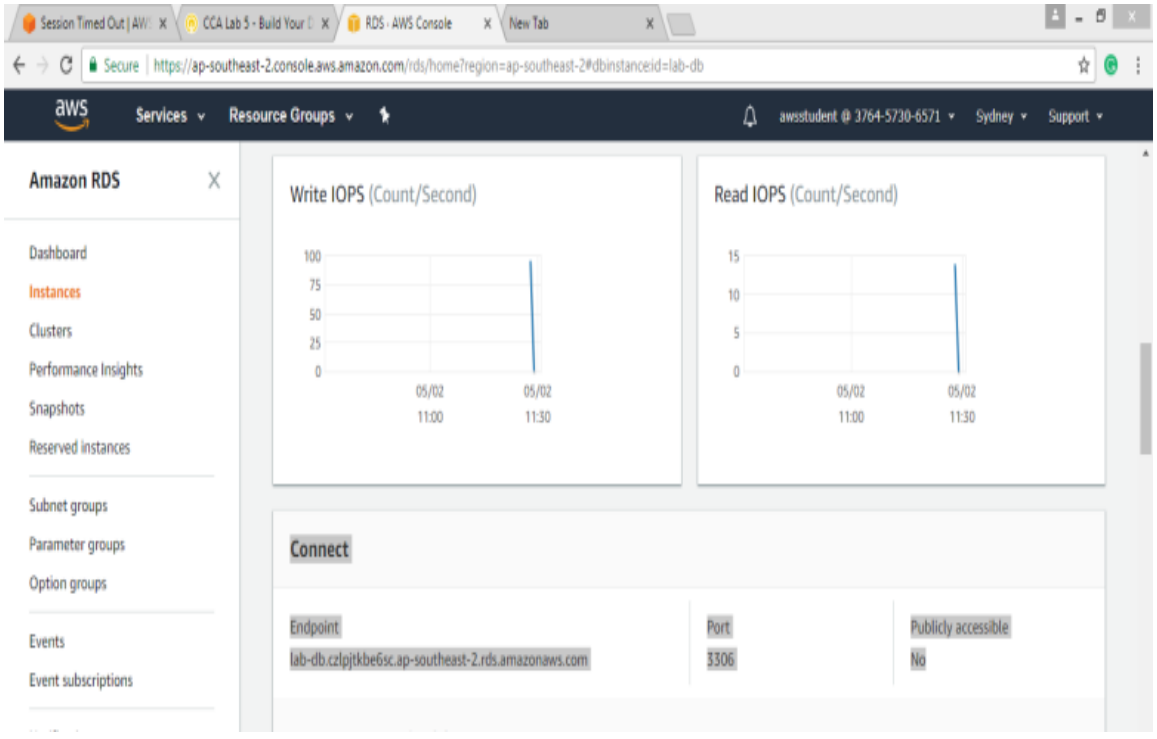


Figure 8.3

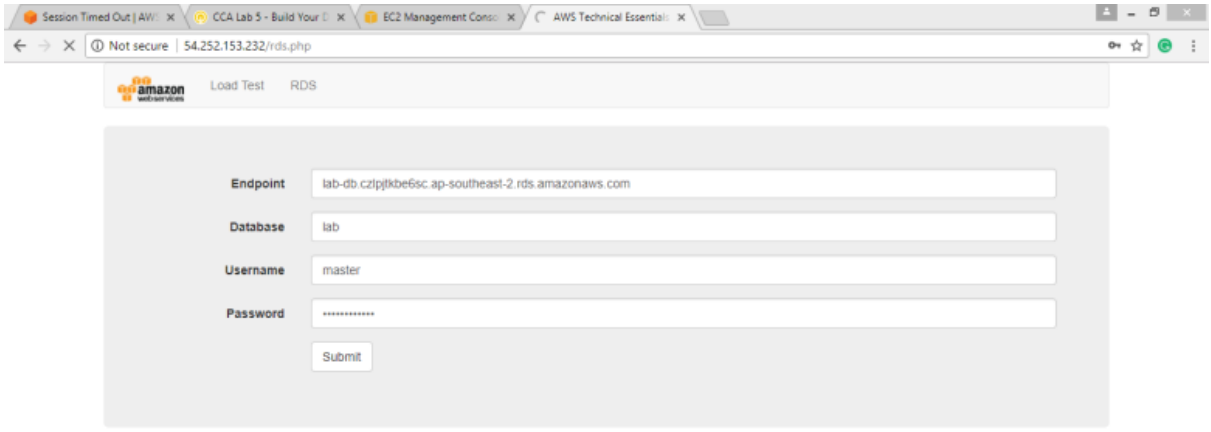


Figure 8.4

- Endpoint: paste endpoint
- Database: lab
- Username: master
- Password: lab-password

A message will have appeared, data have copied in a database and after few minutes Address Book will be displayed on the screen. you can test web application by adding and removing contacts.

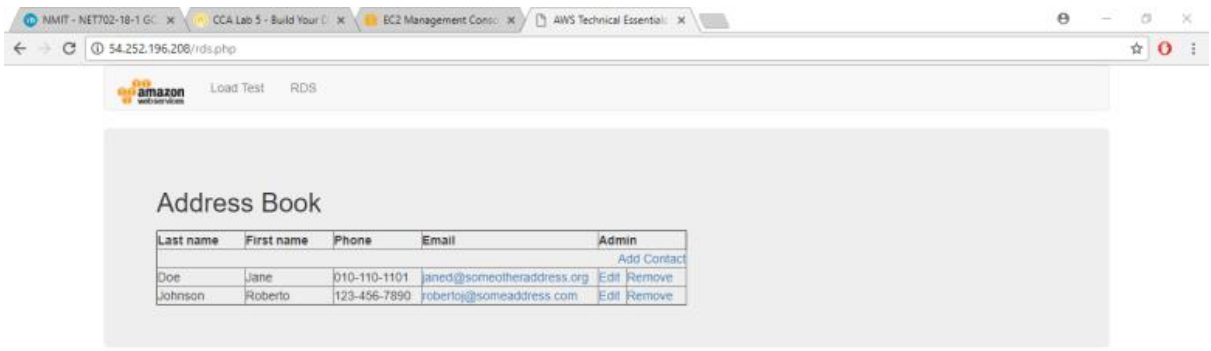


Figure 8.5

Result:

The experiment was successfully executed on AWS free tier in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-9
Date:

Aim: Working on cloud watch

Theory: Amazon CloudWatch is basically a metrics repository. An AWS service—such as Amazon EC2—puts metrics into the repository, and you retrieve statistics based on those metrics. If you put your own custom metrics into the repository, you can retrieve statistics on these metrics as well.

You can configure alarm actions to stop, start, or terminate an Amazon EC2 instance when certain criteria are met. In addition, you can create alarms that initiate Amazon EC2 Auto Scaling and Amazon Simple Notification Service (Amazon SNS) actions on your behalf.

Working:

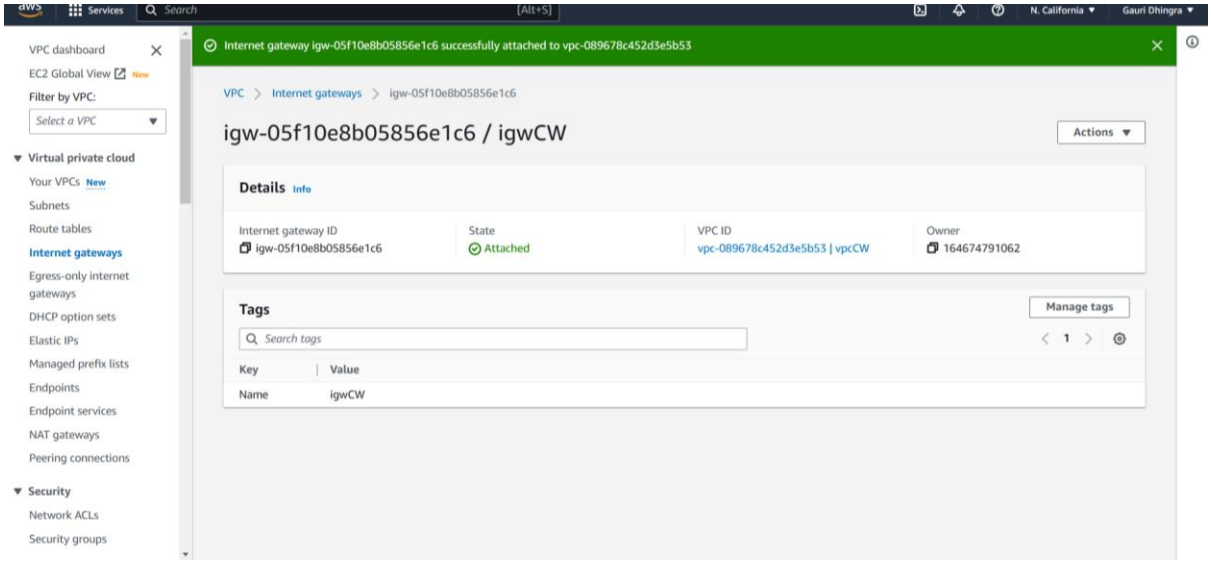


Figure 9.1

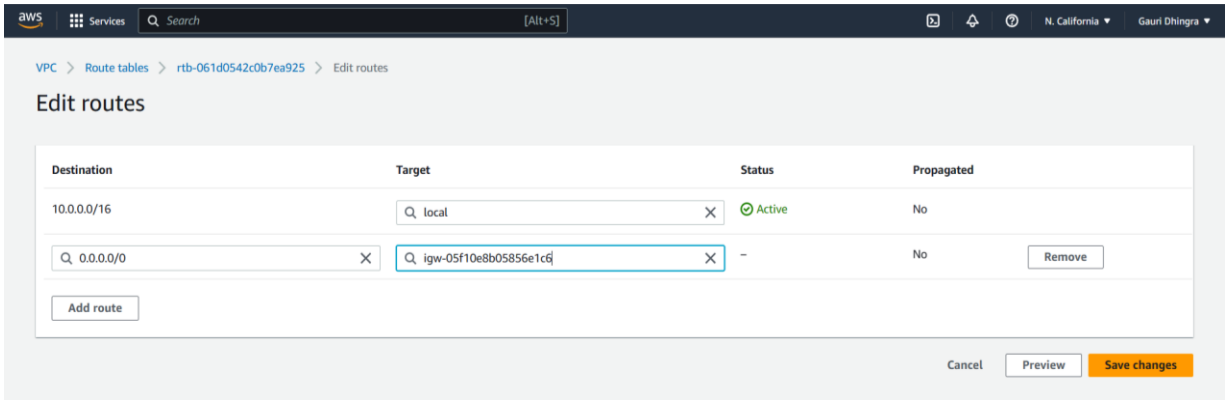


Figure 9.2

After creating VPC, subnet and internet gateway, and routing the subnet click on ec2 launch instance.

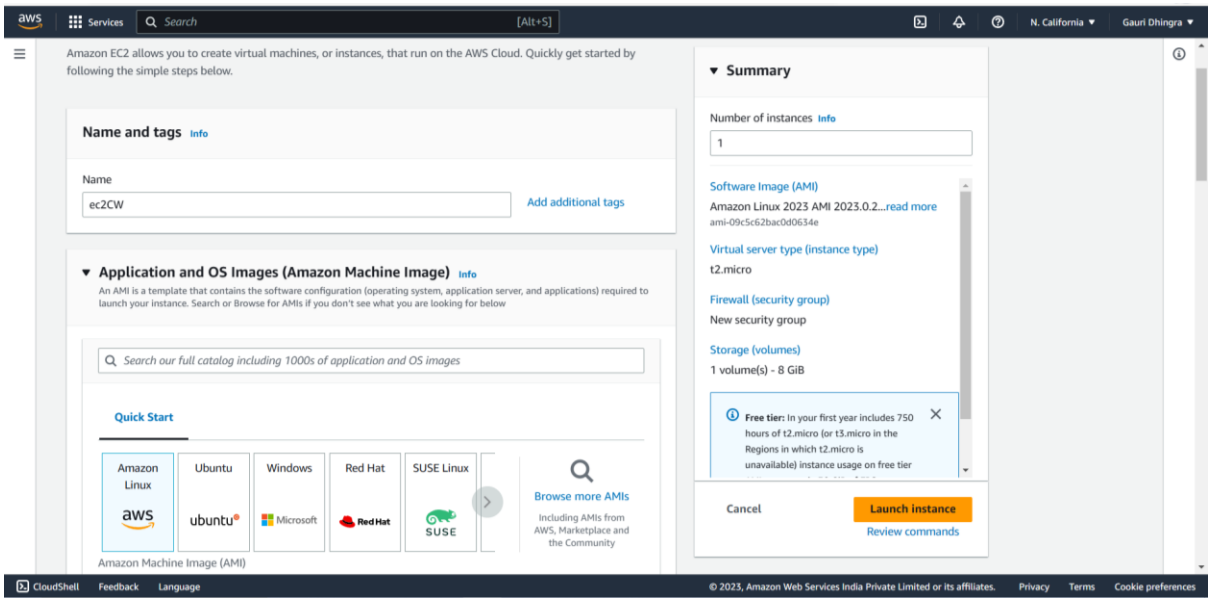


Figure 9.3

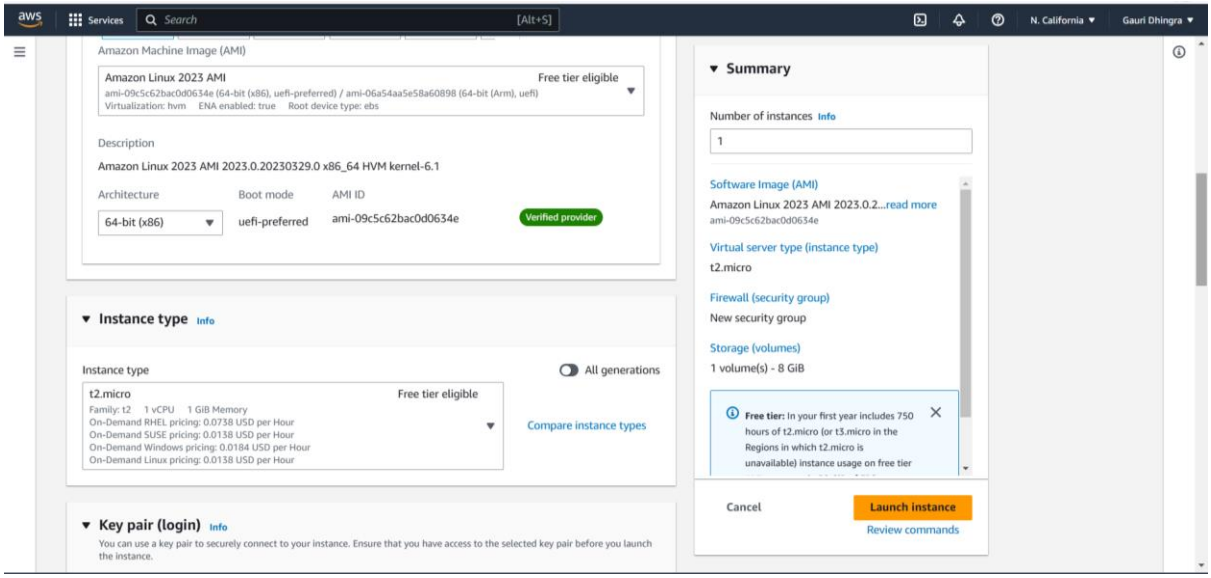


Figure 9.4

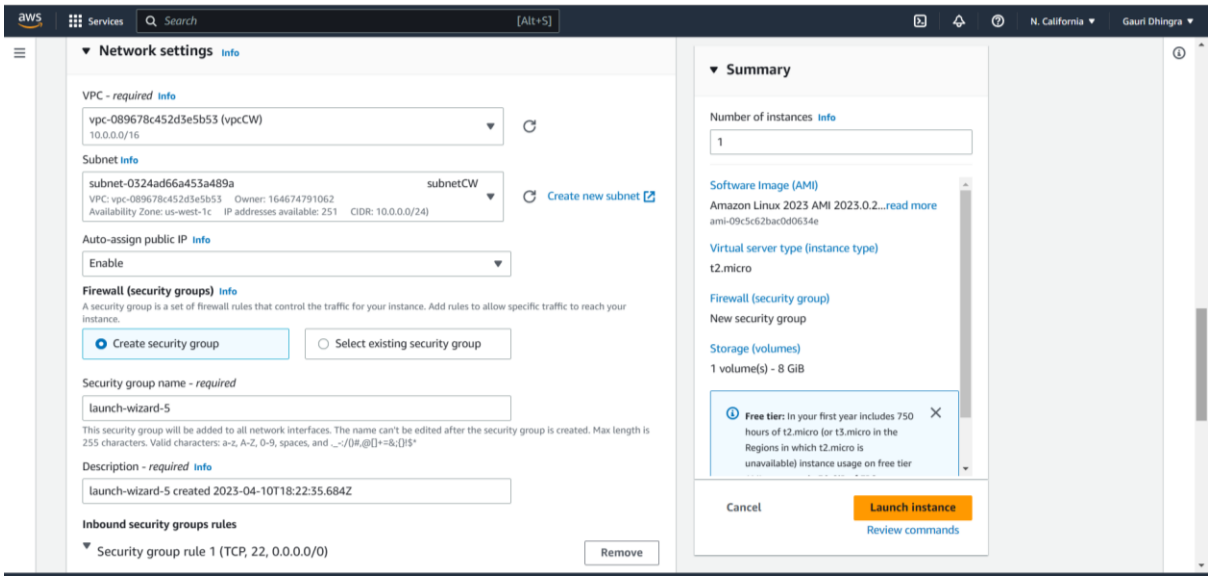


Figure 9.5

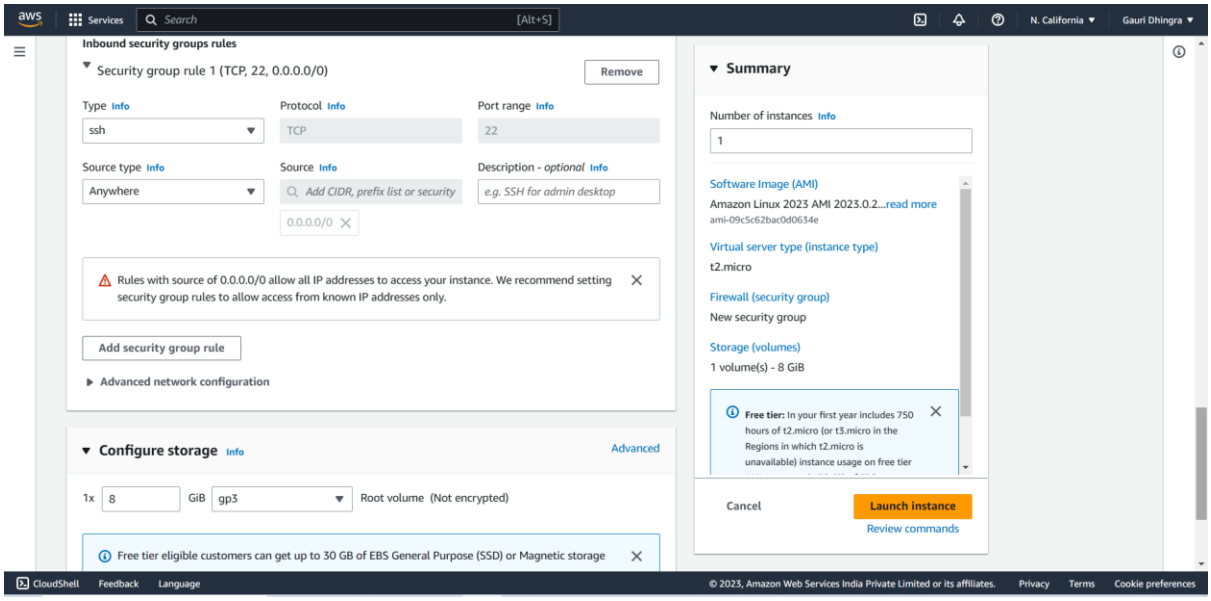


Figure 9.6

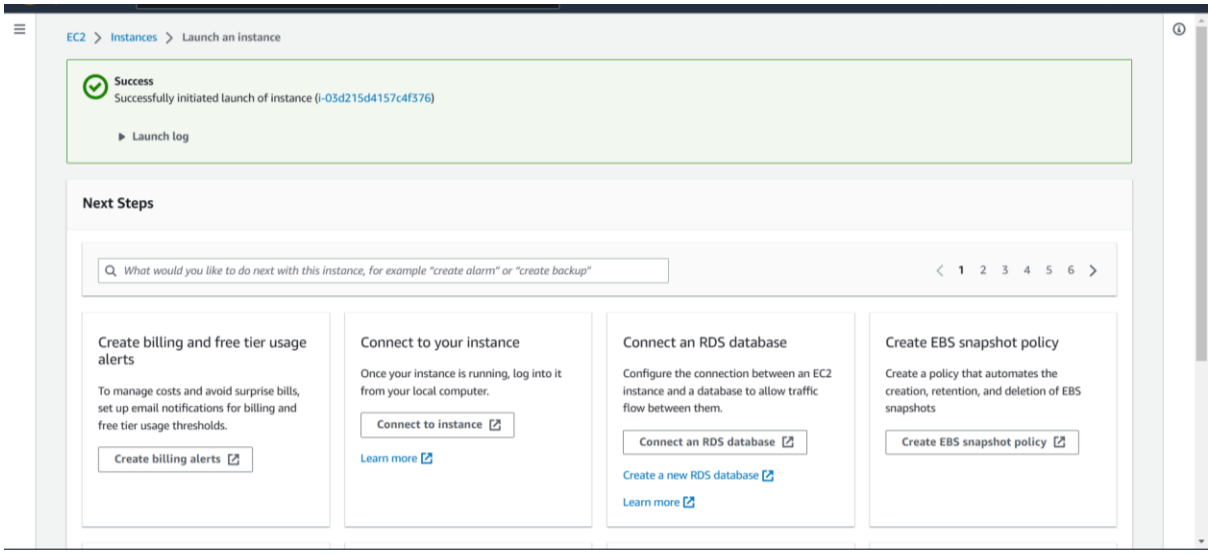


Figure 9.7

Once an ec2 instance is created, create alarm by clicking on + symbol under the alarm status column.

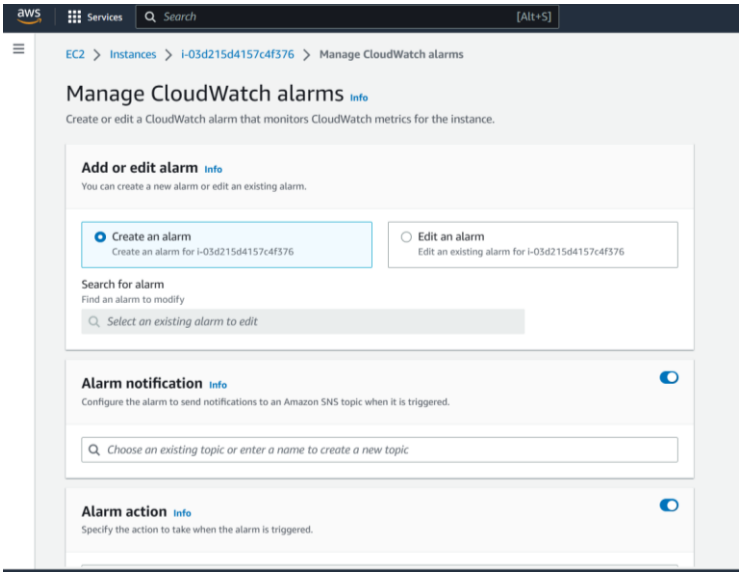


Figure 9.8

In the alarm action select an action out of reboot, stop, terminate, etc. Here I have chosen stop and click on create.

For alarm threshold I have chosen type of data to sample as CPU utilization and percent equal to 0.99.

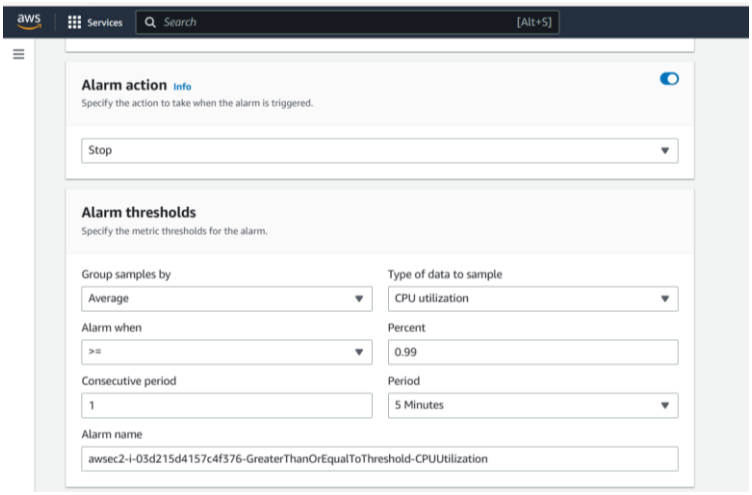


Figure 9.9

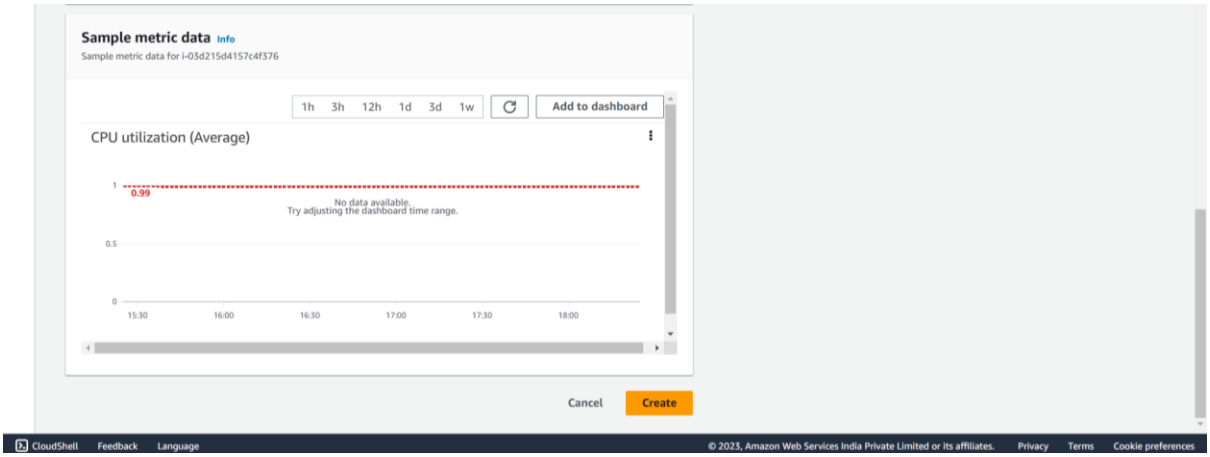


Figure 9.10

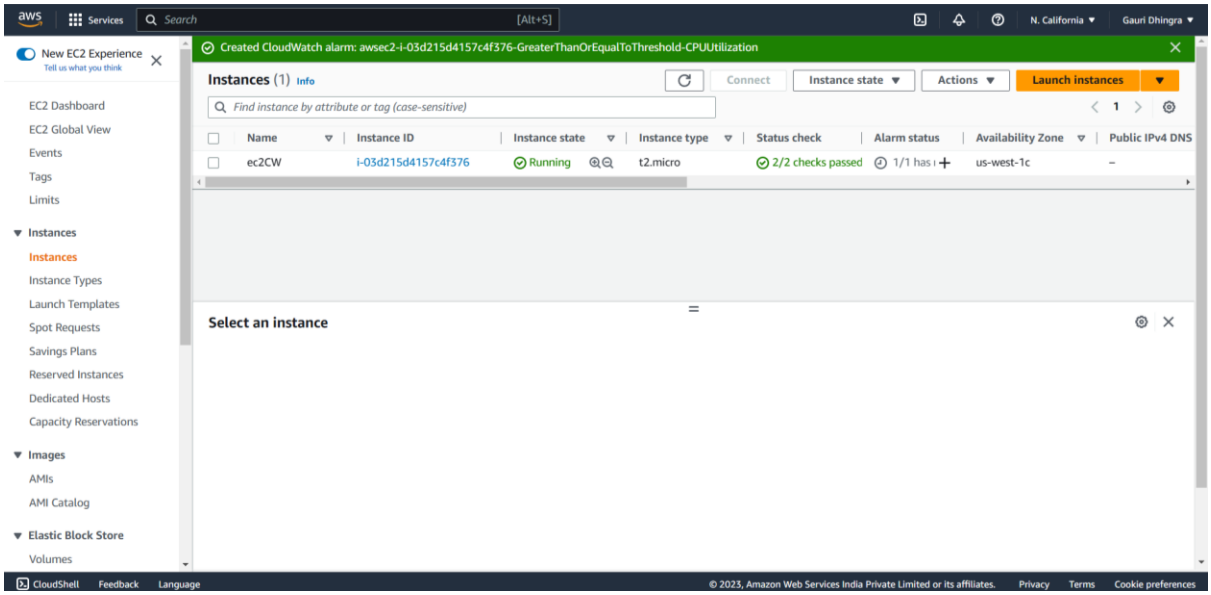


Figure 9.11

Now select the ec2 instance and click on connect.

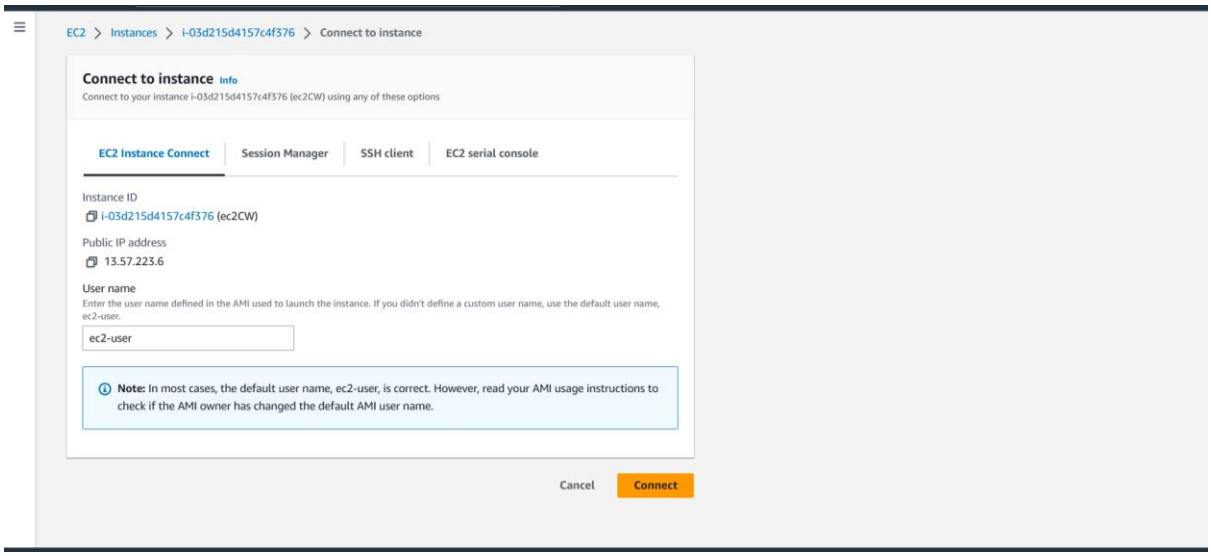


Figure 9.12

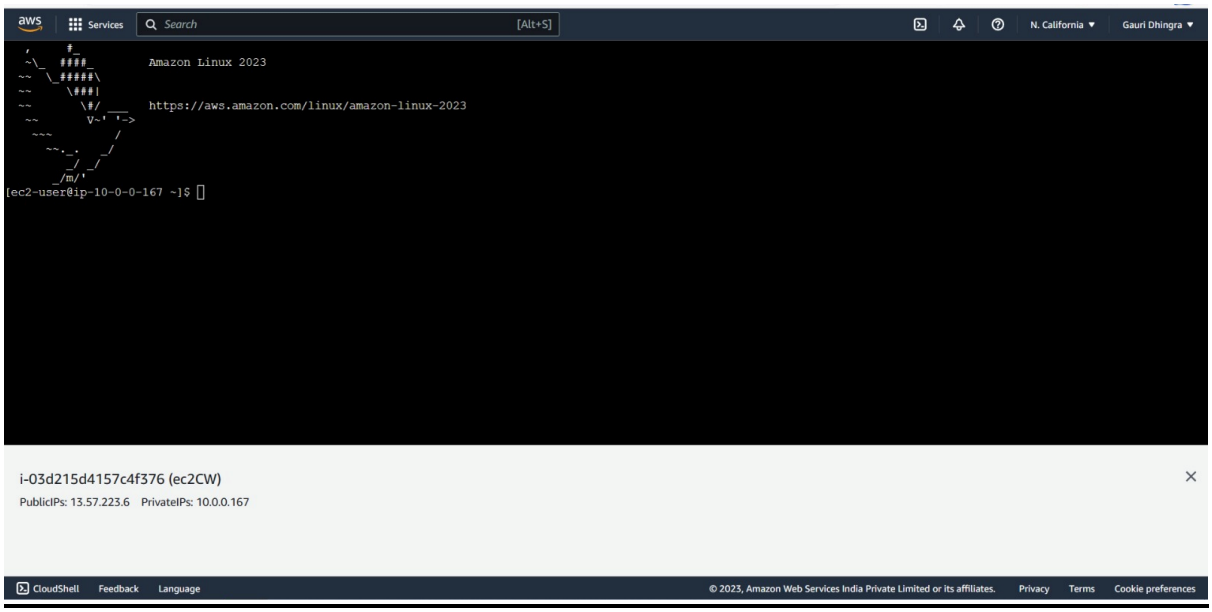


Figure 9.13

After some time, when the threshold of CPU utilization crosses 0.99, the ec2 instance will stop immediately.

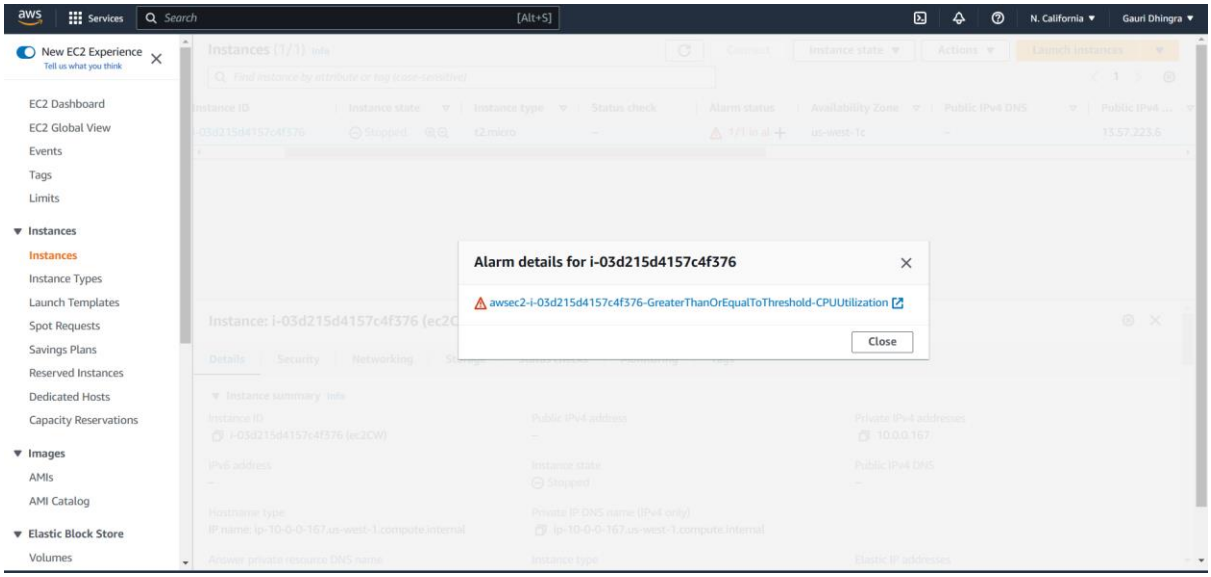


Figure 9.14

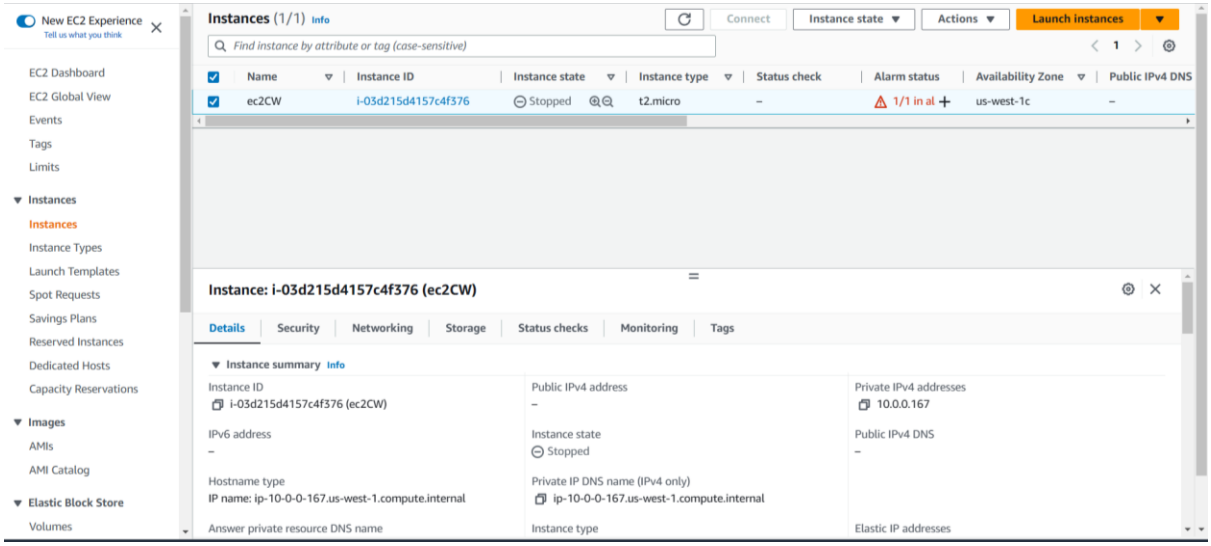


Figure 9.15

Result:

The experiment was successfully executed on AWS free tier in a real-time environment.

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		

Expt.-10
Date:
Aim: Working on cloud trail
Theory:

1. Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/.
2. In the **Region** selector, choose the AWS Region where you want your trail to be created. This is the home Region for the trail.
3. On the CloudTrail service home page, the **Trails** page, or the **Trails** section of the **Dashboard** page, choose **Create trail**.
4. In **Trail name**, give your trail a name, such as *My-Management-Events-Trail*. As a best practice, use a name that quickly identifies the purpose of the trail. In this case, you're creating a trail that logs management events.

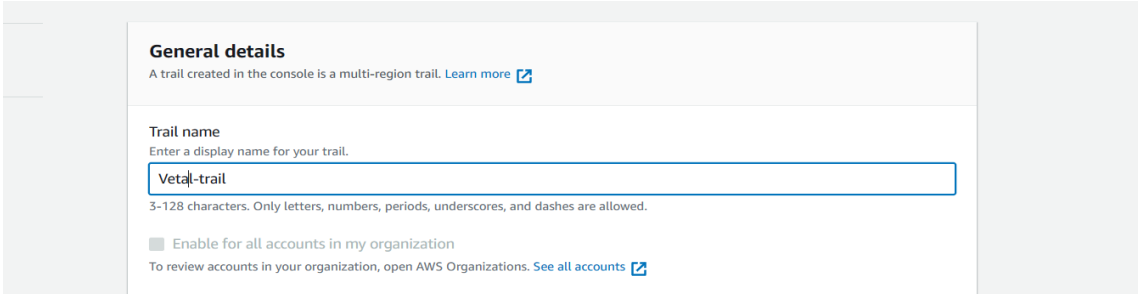


Figure 10.1

5. Leave default settings for AWS Organizations organization trails. This option won't be available to change unless you have accounts configured in Organizations.
6. For **Storage location**, choose **Create new S3 bucket** to create a bucket. When you create a bucket, CloudTrail creates and applies the required bucket policies. Give your bucket a name, such as *my-bucket-for-storing-cloudtrail-logs*.

To make it easier to find your logs, create a new folder (also known as a *prefix*) in an existing bucket to store your CloudTrail logs. Enter the prefix in **Prefix**.

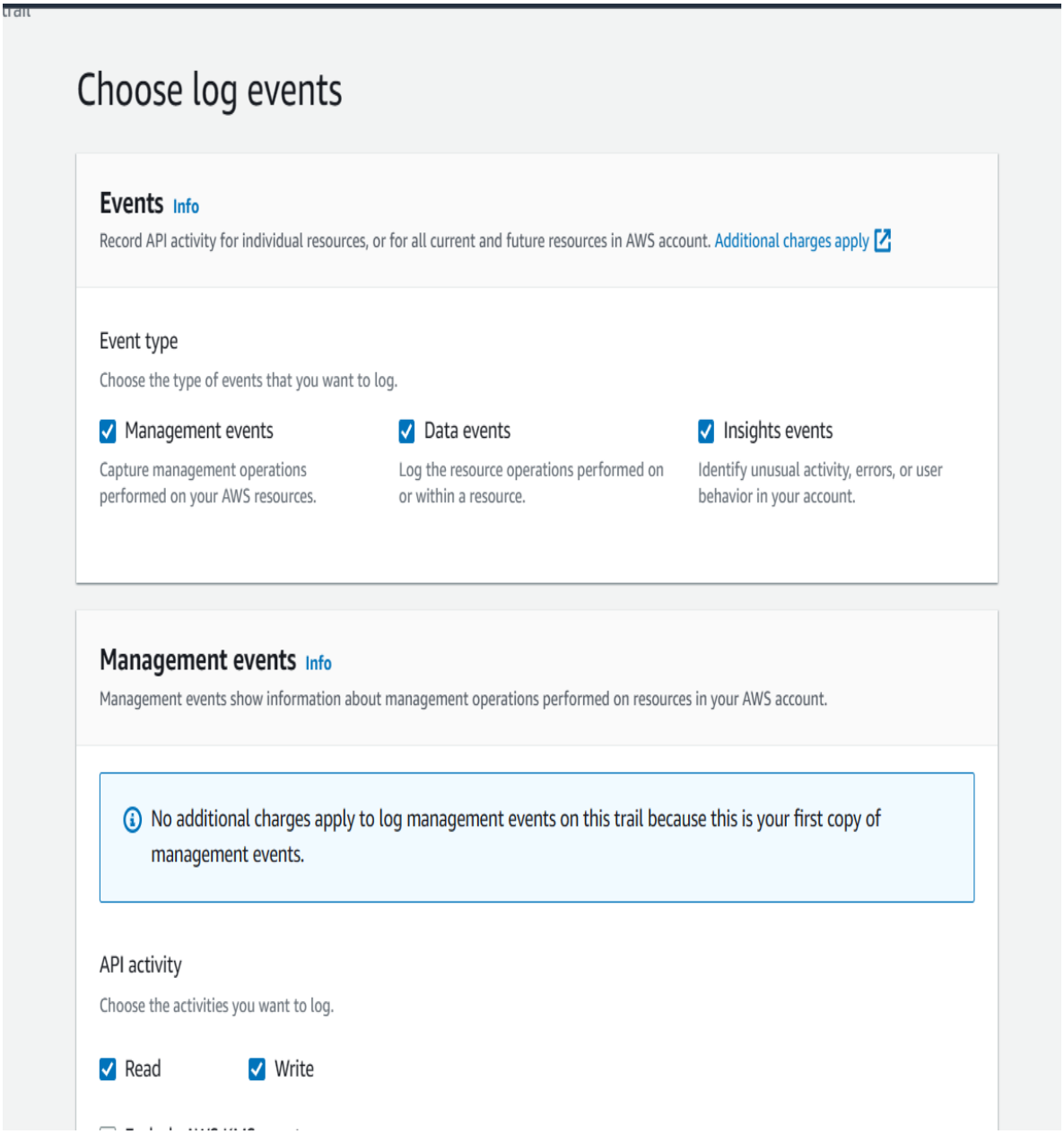

Choose log events
Events Info
Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply
Event type
Choose the type of events that you want to log.
Management events
Capture management operations performed on your AWS resources.
Data events
Log the resource operations performed on or within a resource.
Insights events
Identify unusual activity, errors, or user behavior in your account.
Management events Info
Management events show information about management operations performed on resources in your AWS account.
No additional charges apply to log management events on this trail because this is your first copy of management events.
API activity
Choose the activities you want to log.
Read
Write

Figure 10.2

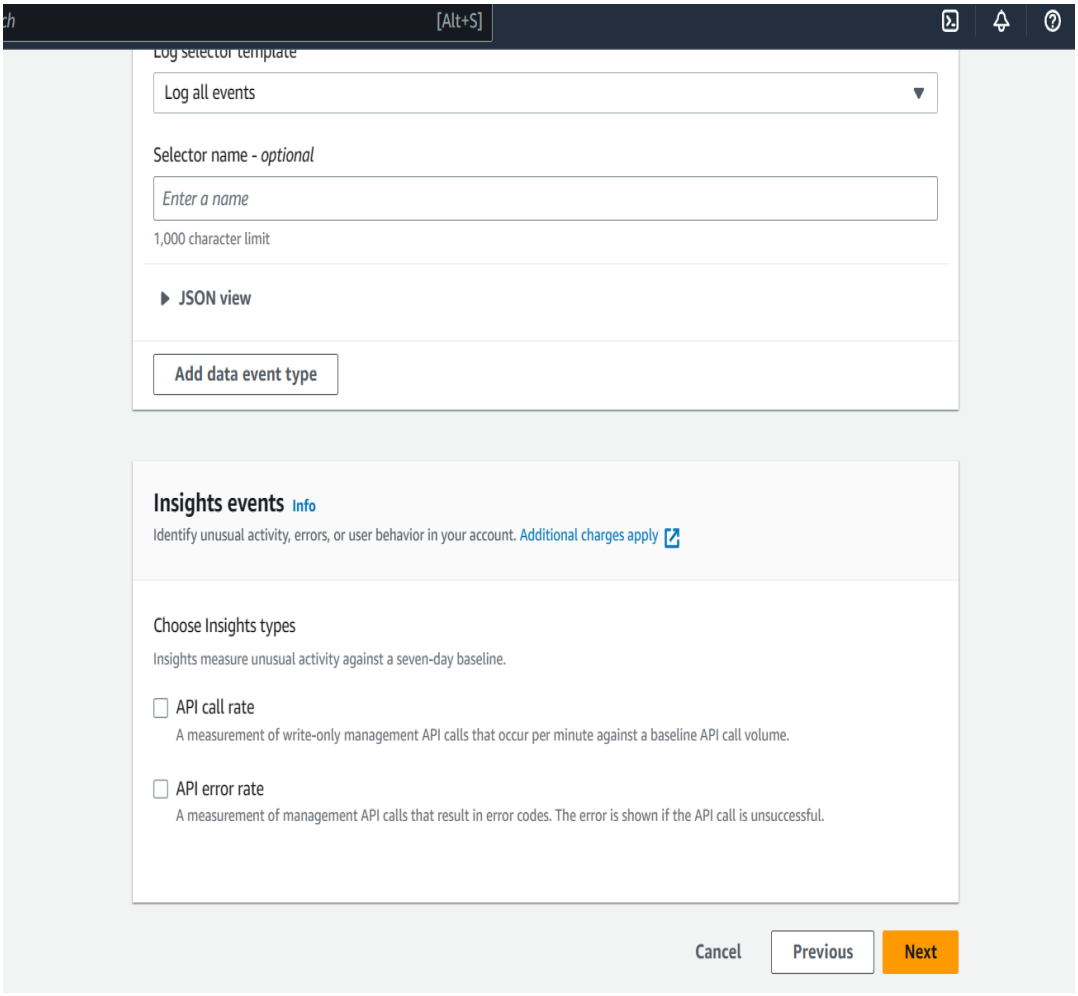


Figure 10.3

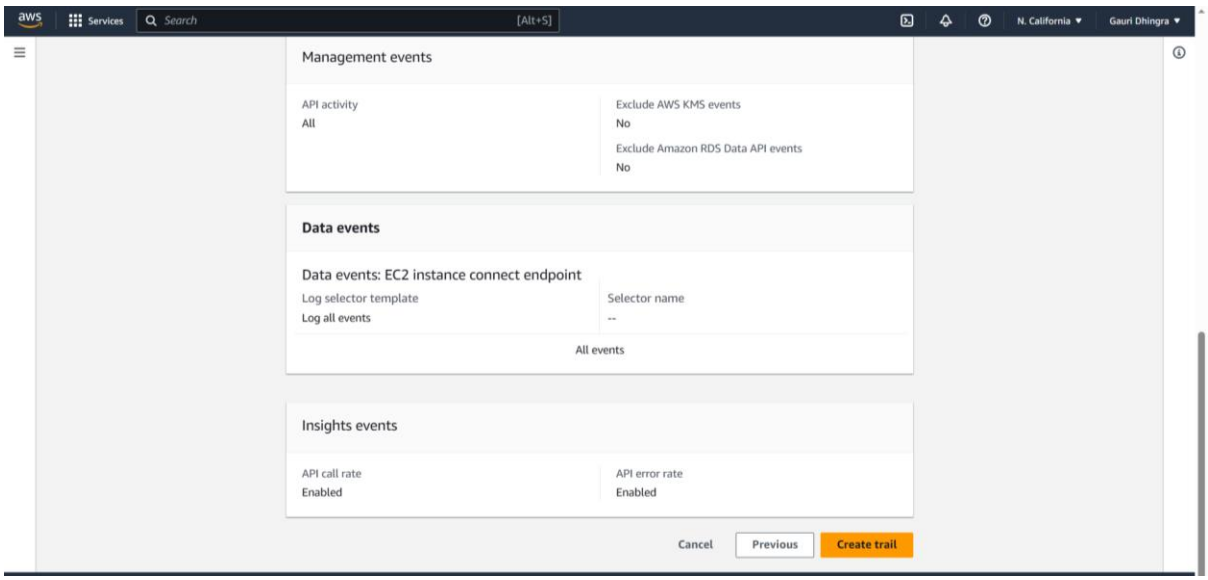


Figure 10.4

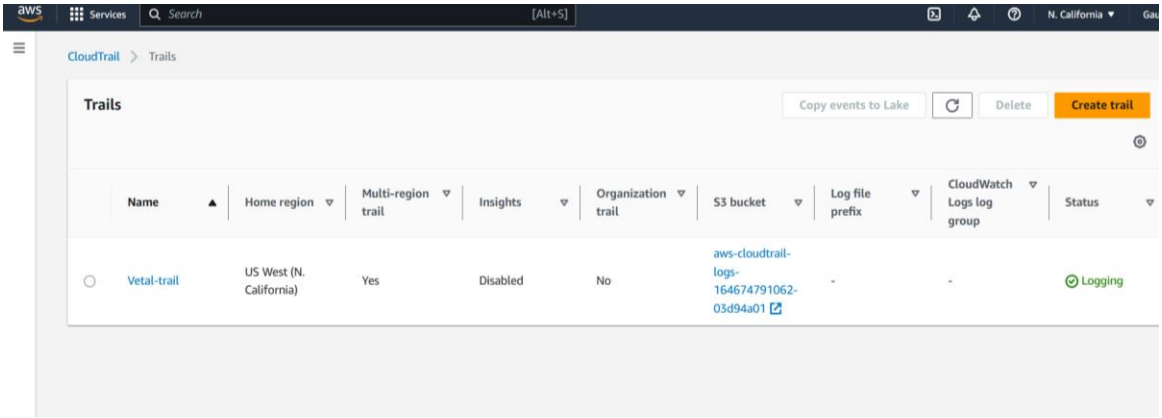


Figure 10.5

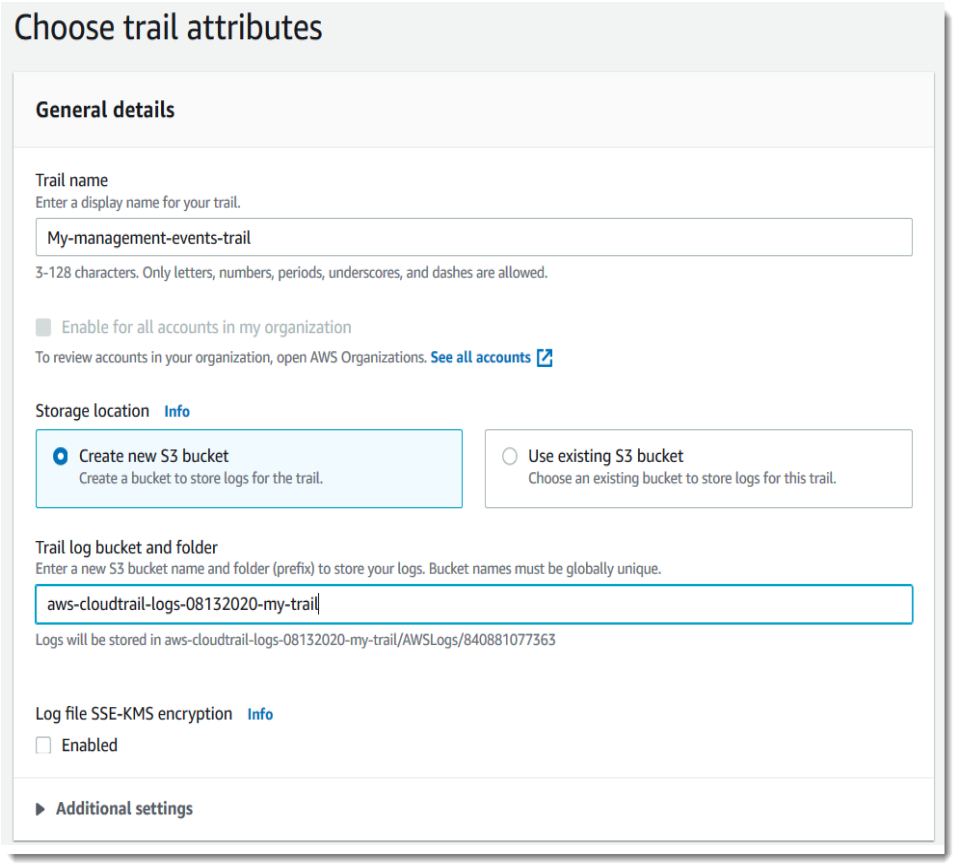


Figure 10.6

7. Clear the check box to disable **Log file SSE-KMS encryption**. By default, your log files are encrypted with SSE-S3 encryption. For more information about this setting, see Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys (SSE-S3).
8. Leave default settings in **Additional settings**.

9. For now, do not send logs to Amazon CloudWatch Logs.
10. In **Tags**, add one or more custom tags (key-value pairs) to your trail. Tags can help you identify your CloudTrail trails and other resources, such as the Amazon S3 buckets that contain CloudTrail log files. For example, you could attach a tag with the name **Compliance** and the value **Auditing**.

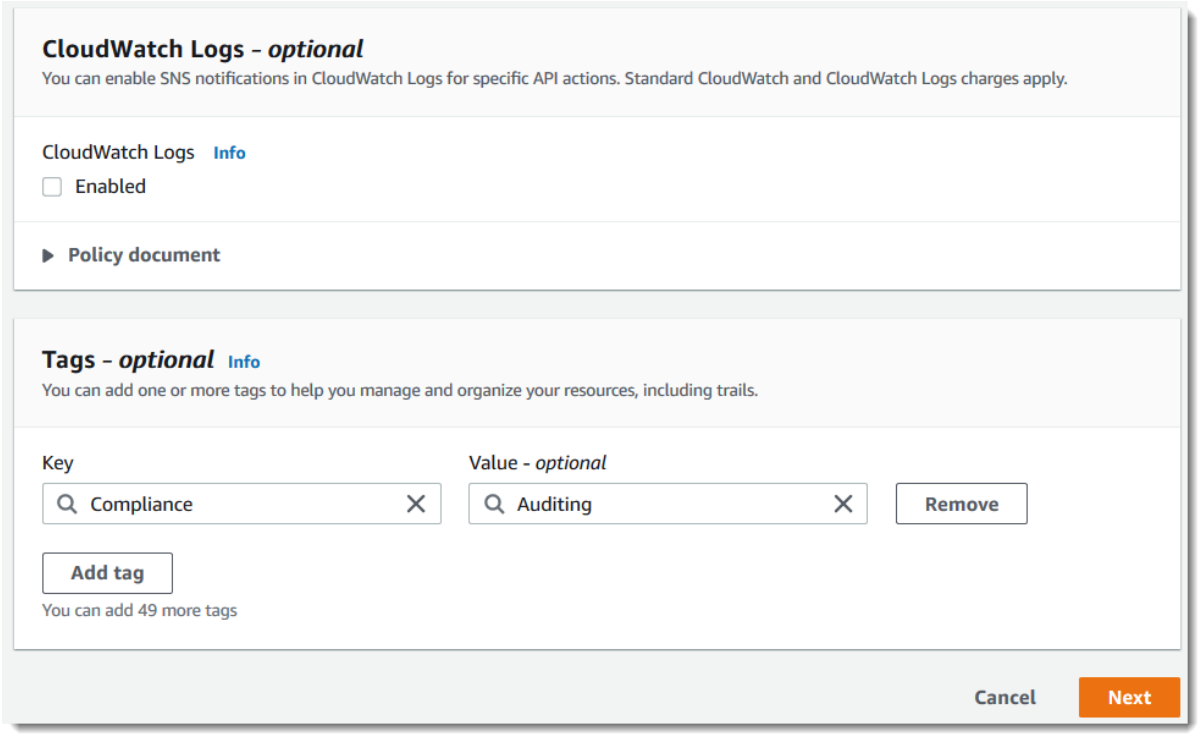


Figure 10.7

When you are finished creating tags, choose **Next**.

11. On the **Choose log events** page, select event types to log. For this trail, keep the default, **Management events**. In the **Management events** area, choose to log both **Read** and **Write** events, if they are not already selected. Leave the check boxes for **Exclude AWS KMS events** and **Exclude Amazon RDS Data API events** empty, to log all events.

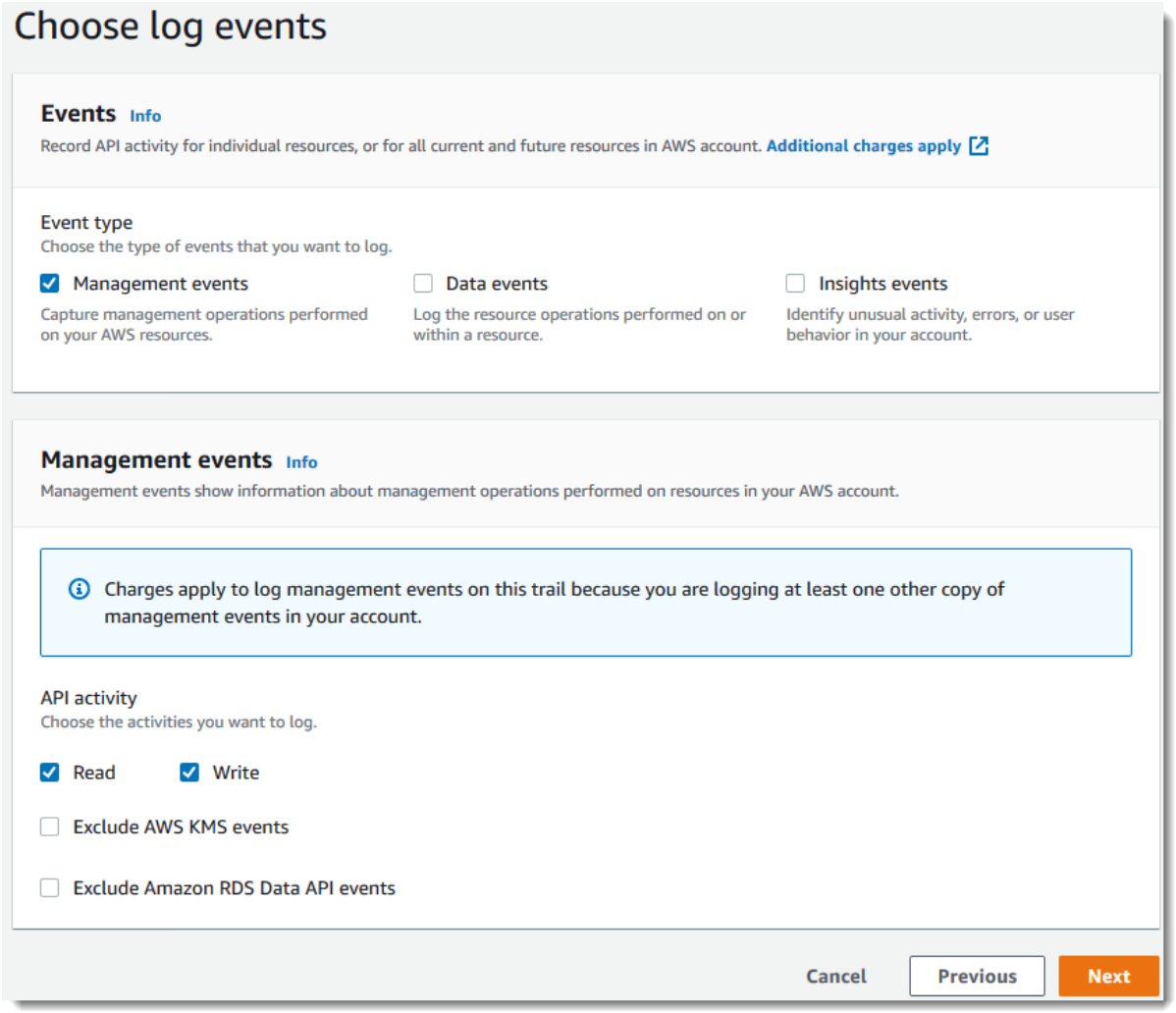


Figure 10.8

12. Leave default settings for **Data events** and Insights events. This trail will not log any data or CloudTrail Insights events. Choose **Next**.
13. On the **Review and create** page, review the settings you've chosen for your trail. Choose **Edit** for a section to go back and make changes. When you are ready to create your trail, choose **Create trail**.
14. The **Trails** page shows your new trail in the table. Note that the trail is set to **Multi-region trail** by default, and that logging is turned on for the trail by default.

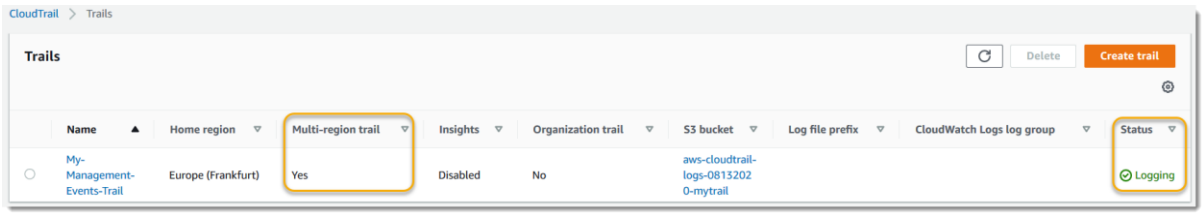


Figure 10.9

Internal Assessment (Mandatory Experiment) Sheet for Lab Experiment Department of Computer Science & Engineering Amity University, Noida (UP)			
Programme	B. Tech CSE	Course Name	Cloud Computing Practitioner
Course Code	[CSE-314]	Semester	6
Student Name	Gauri Dhingra	Enrollment No.	A2305220310
Marking Criteria			
Criteria	Total Marks	Marks Obtained	Comments
Concept (A)	2		
Implementation (B)	2		
Performance (C)	2		
Total	6		