

## Lab Assignment – 02

### Lab 2 of AWS Academy Foundations course.

#### Objectives:

- 1) Create a VPC
- 2) Create Subnets
- 3) Configure a security group
- 4) Launch an EC2 instance into VPC

#### Task-1: Create your VPC

Lab 2 - Build your VPC and Launch an EC2 Instance

VPC Management Console

https://console.aws.amazon.com/vpc/home?region=us-east-1#wizardSelector

Services Search for services, features, marketplace products, and docs [Alt+S]

voclabs/user1191784-MV3451@bennett.edu.in @ 7737-2525-0502 N. Virginia Support

#### Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

**VPC with Public and Private Subnets**

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).

**Creates:**

A /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via Network Address Translation (NAT). (Hourly charges for NAT devices apply.)

**Important:**  
If you are using a Local Zone with your VPC follow this link to create your VPC.

Select

Cancel and Exit

Internet S3, DynamoDB, SNS, SQS, etc.

Amazon Virtual Private Cloud

Public Subnet NAT Private Subnet

Feedback English (US) © 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

09:56 27-01-2021

## 1) Setting up 2 subnets (1 public + 1 private)

The screenshot shows the AWS VPC Management Console interface. The browser address bar displays the URL: `https://console.aws.amazon.com/vpc/home?region=us-east-1#wizardFullpagePublicAndPrivate`. The page title is "Step 2: VPC with Public and Private Subnets".

Configuration details visible on the page:

- IPv4 CIDR block:** 10.0.0.0/16 (65531 IP addresses available)
- IPv6 CIDR block:** ☒ No IPv6 CIDR Block
  - ☐ Amazon provided IPv6 CIDR block
  - ☐ IPv6 CIDR block owned by me
- VPC name:** Lab VPC
- Public subnet's IPv4 CIDR:** 10.0.0.0/24 (251 IP addresses available)
  - Availability Zone:** us-east-1a
  - Public subnet name:** Public Subnet 1
- Private subnet's IPv4 CIDR:** 10.0.1.0/24 (251 IP addresses available)
  - Availability Zone:** us-east-1a
  - Private subnet name:** Private Subnet 1
- Elastic IP Allocation ID:** eipalloc-01dadb0974d8d9b4
- Service endpoints:** Add Endpoint

At the bottom, there is a footer with "Feedback", "English (US)", and copyright information: "© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved." along with "Privacy Policy" and "Terms of Use" links.

The wizard has provisioned a VPC with a public subnet and a private subnet in the same Availability Zone, together with route tables for each subnet.

## Task-2: Create additional subnets

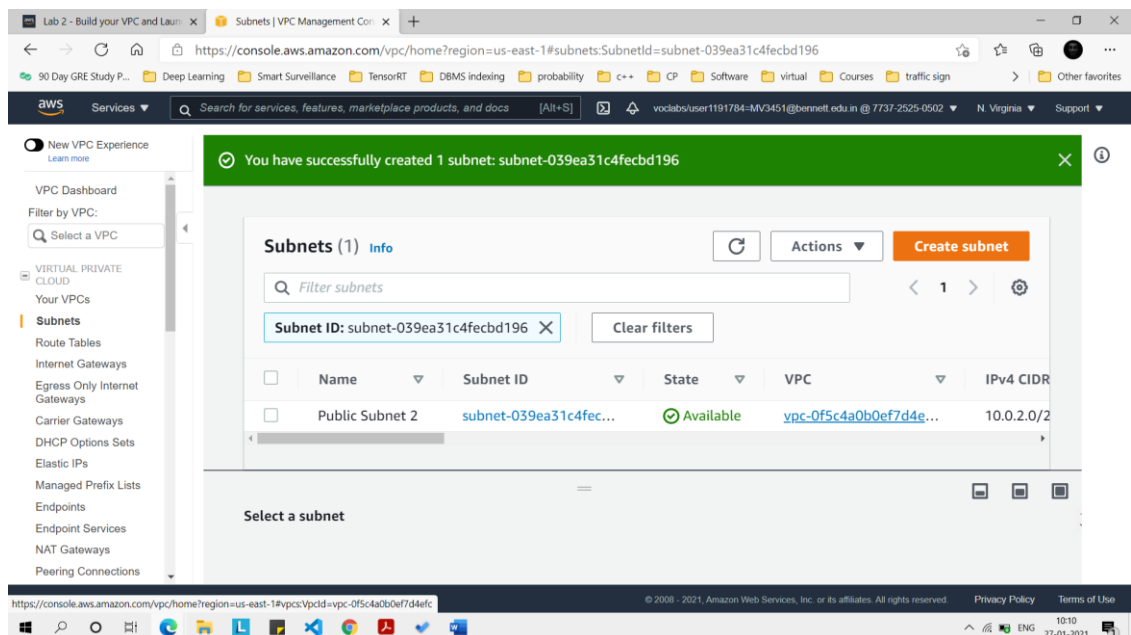
### 1) Create 2 additional subnets in the second availability zone.

The screenshot shows the AWS VPC Management Console interface for creating a new subnet. The browser address bar displays the URL: `https://console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet`. The page title is "Specify the CIDR blocks and Availability Zone for the subnet."

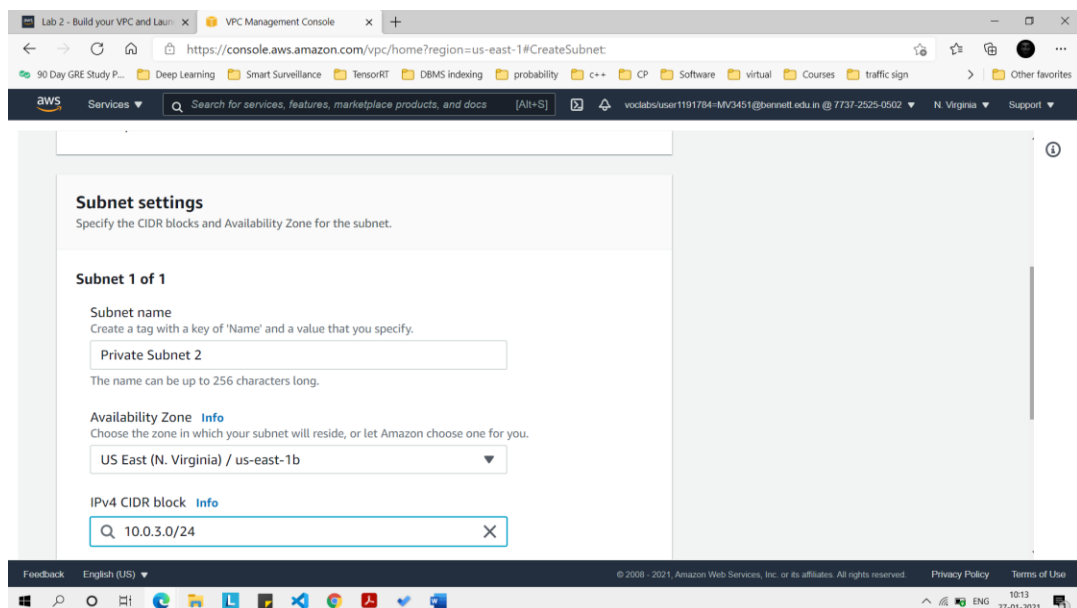
Configuration details visible on the page:

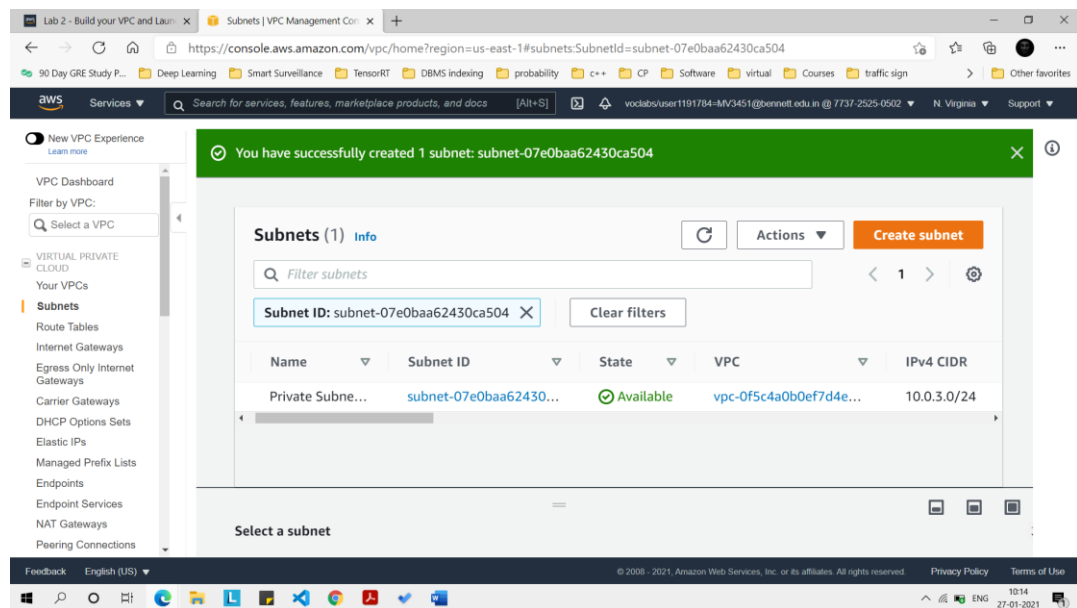
- Subnet 1 of 1**
- Subnet name:** Create a tag with a key of 'Name' and a value that you specify.
  - Public Subnet 2**
  - The name can be up to 256 characters long.
- Availability Zone:** [Info](#)
  - Choose the zone in which your subnet will reside, or let Amazon choose one for you.
  - US East (N. Virginia) / us-east-1b**
- IPv4 CIDR block:** [Info](#)
  - 10.0.2.0/24**
- Tags - optional**
  - Key:** Name
  - Value - optional:** Public Subnet 2
  - Remove**

At the bottom, there is a footer with "Feedback", "English (US)", and copyright information: "© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved." along with "Privacy Policy" and "Terms of Use" links.



2) Now create second Private Subnet 2 in the same second availability zone.





You will now configure the Private subnets to route internet-bound traffic to the NAT Gateway so that the resources in the private subnet are able to connect to the internet, while 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 the network traffic is directed.

Each subnet in a VPC must be associated with a route table, the route table controls routing for the subnet.

3) Configure the Route Table used by private subnets.

The screenshot shows the 'Edit subnet associations' page in the AWS Management Console. The route table is 'rtb-0d5706b107aa57' (Private Route Table). The associated subnets are 'subnet-07e0baa62430ca504' and 'subnet-0d1c1fd28c7707a7b'. A table lists the subnets and their associated route tables:

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-039ea31c4fecbd196   Public Subnet 2	10.0.2.0/24	-	Main
subnet-07e0baa62430ca504   Private Subnet 2	10.0.3.0/24	-	Main
subnet-0d1c1fd28c7707a7b   Private Subnet 1	10.0.1.0/24	-	Main
subnet-00db59e2466adc232   Public Subnet 1	10.0.0.0/24	-	rtb-0c5cf59d1580be88f

Buttons for 'Cancel' and 'Save' are visible at the bottom right.

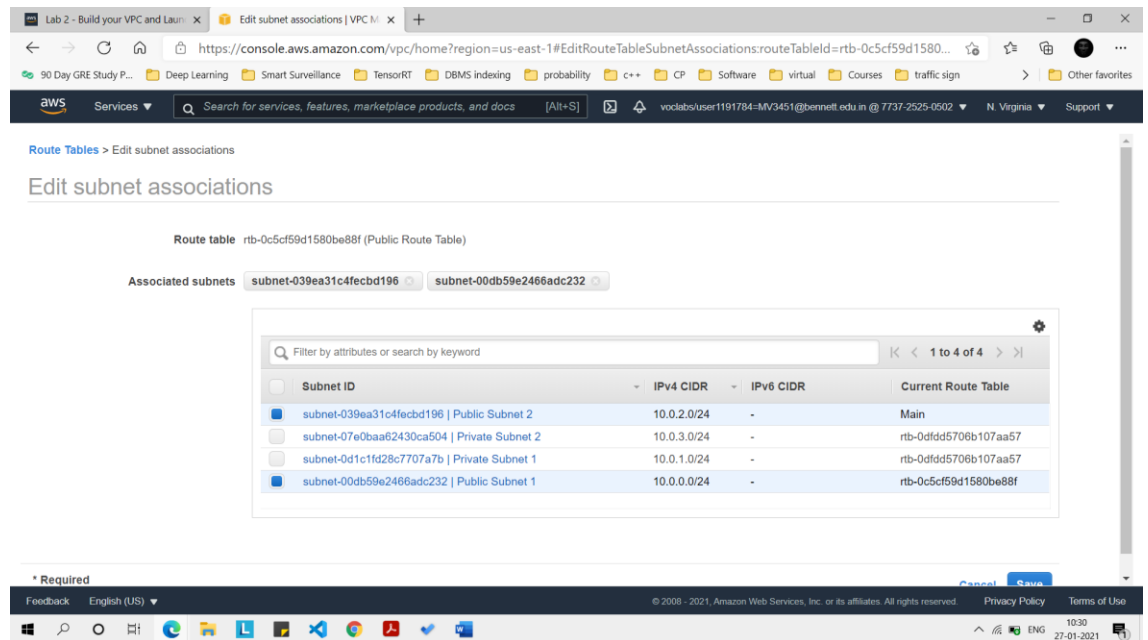
#### 4) Configure the Route Table used by public subnets.

The screenshot shows the 'Route Tables' page in the AWS Management Console. A table lists the route tables:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
Public Route Table	rtb-0c5cf59d1580be88f	subnet-00db59e2466adc232	-	No	vpc-0f5c4a0b0ef7d4efc   L
Private Route Table	rtb-0d5706b107aa57	2 subnets	-	Yes	vpc-0f5c4a0b0ef7d4efc   L
	rtb-3bc2ef45	-	-	Yes	vpc-5173d52c

The 'Route Table: rtb-0c5cf59d1580be88f' is selected, and the 'Routes' tab is active. The routes table shows:

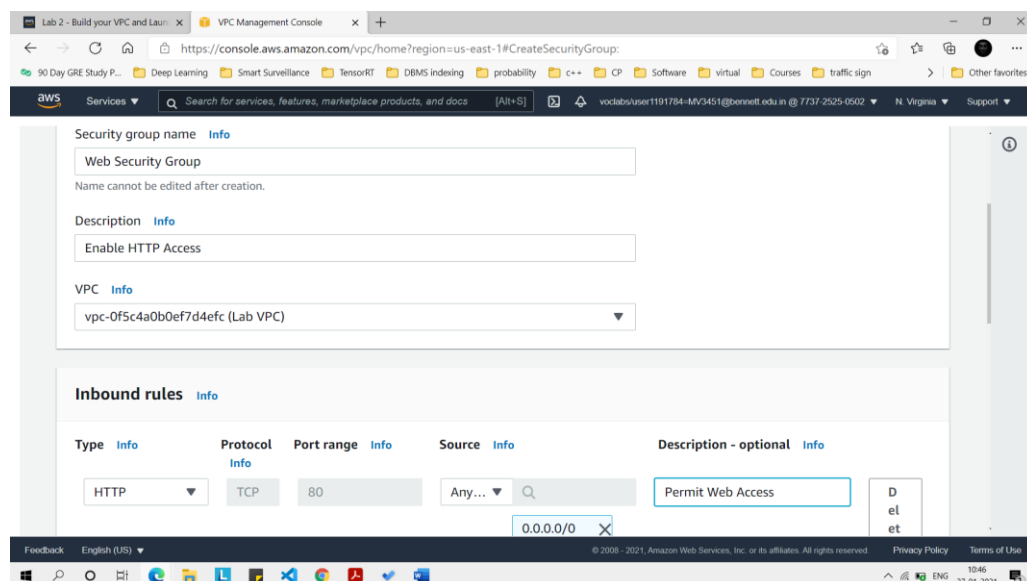
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-08e25c55e5885b6f1	active	No

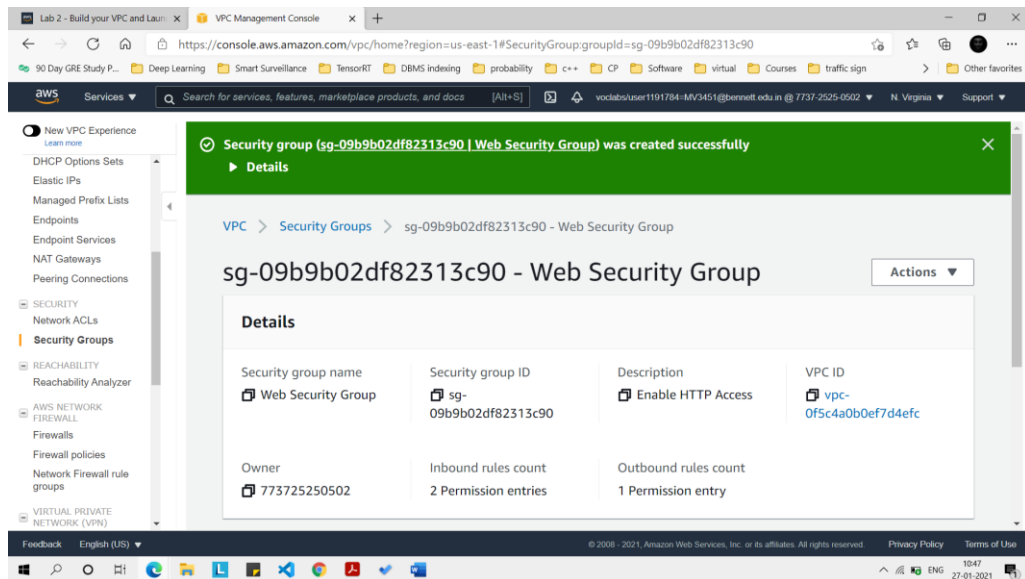


Your VPC now has public and private subnets configured in 2 availability zones.

### Task-3: Create a VPC Security Group

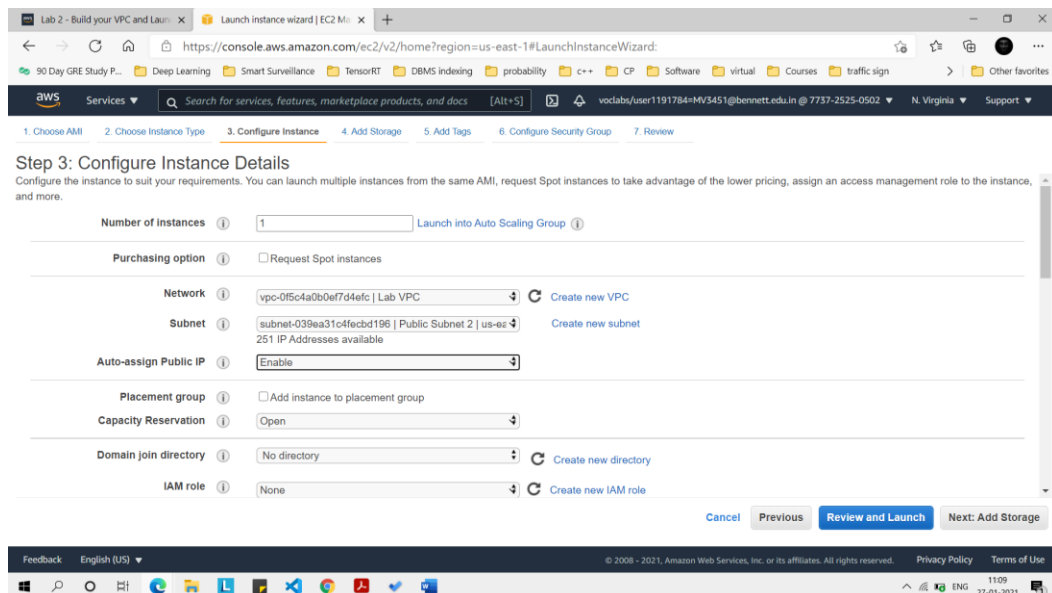
1) Create a VPC Security Group which acts as a virtual firewall

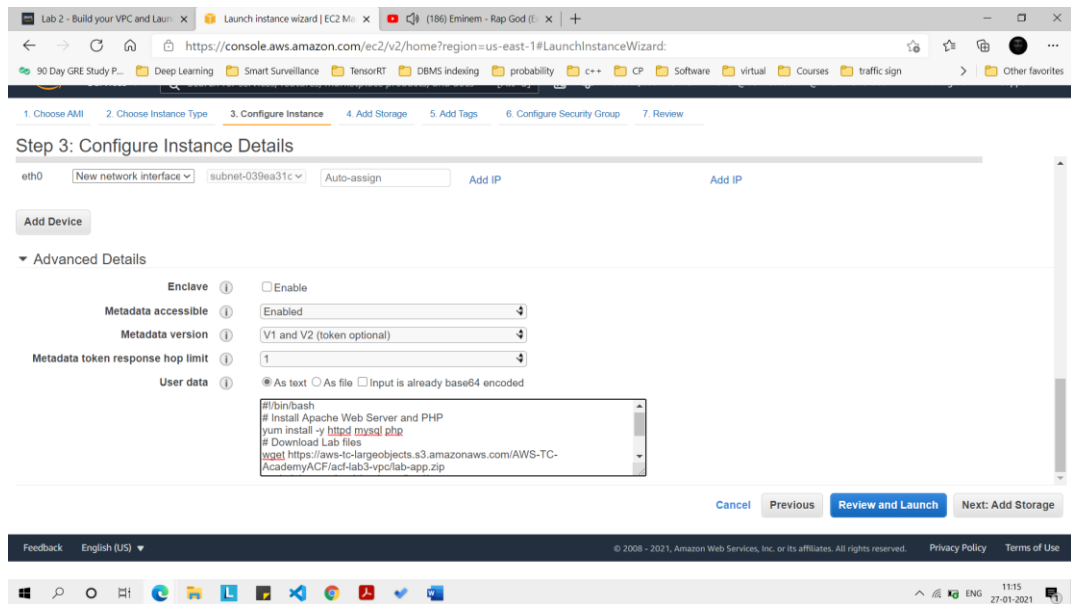




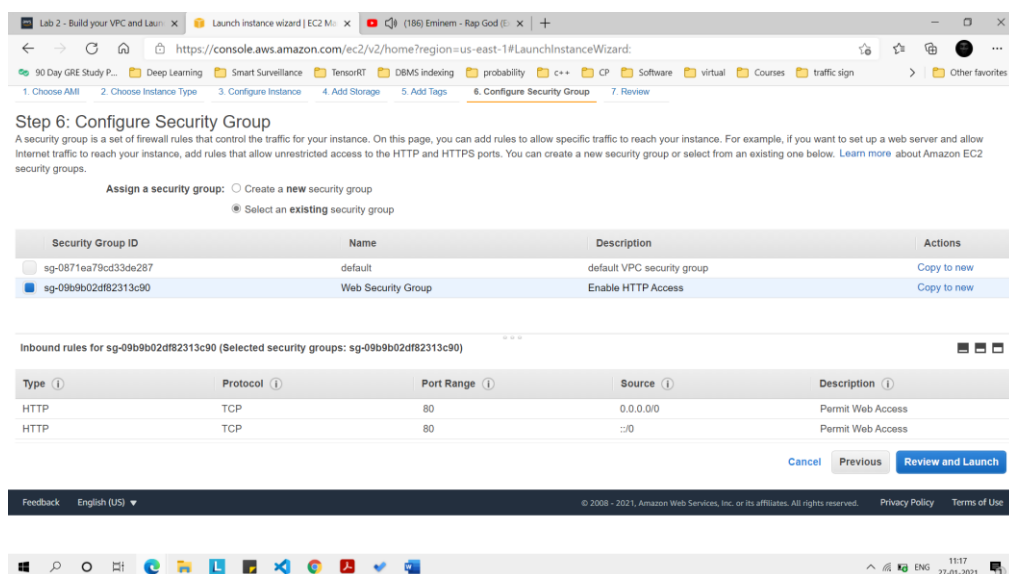
## Task-4: Launch a Web Server Instance

- 1) Configure the instance to launch in a public subnet of the new VPC



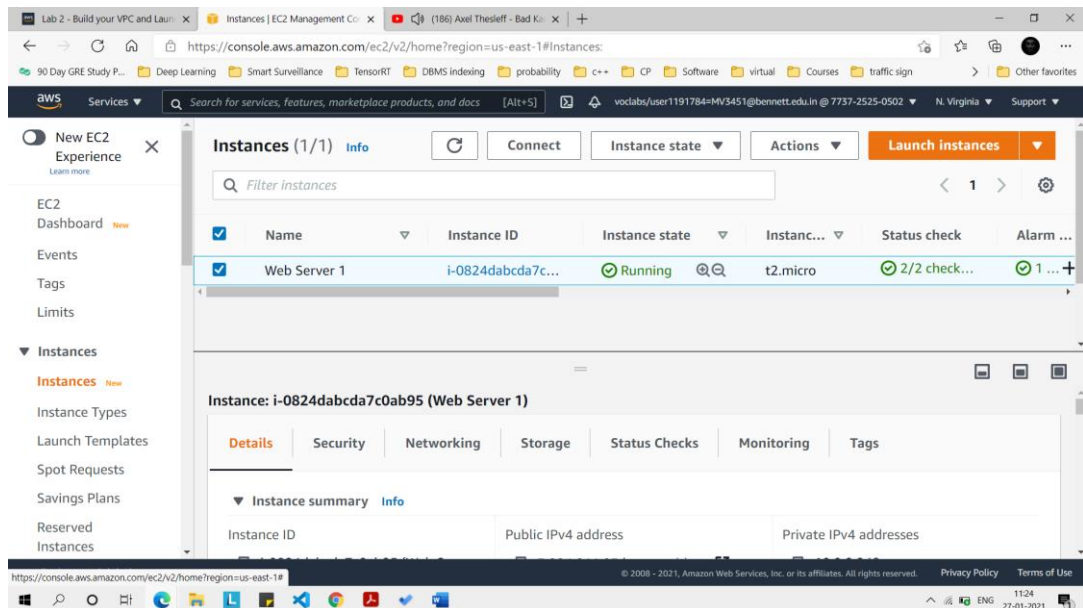


2) Use the security group created earlier.



3) The instance is now successfully running in the public subnet of your VPC





Final Confirmation of the working of the server. The below HTTP request results in a success and we are able to see a webpage showing the AWS logo and the instance meta-data values.

