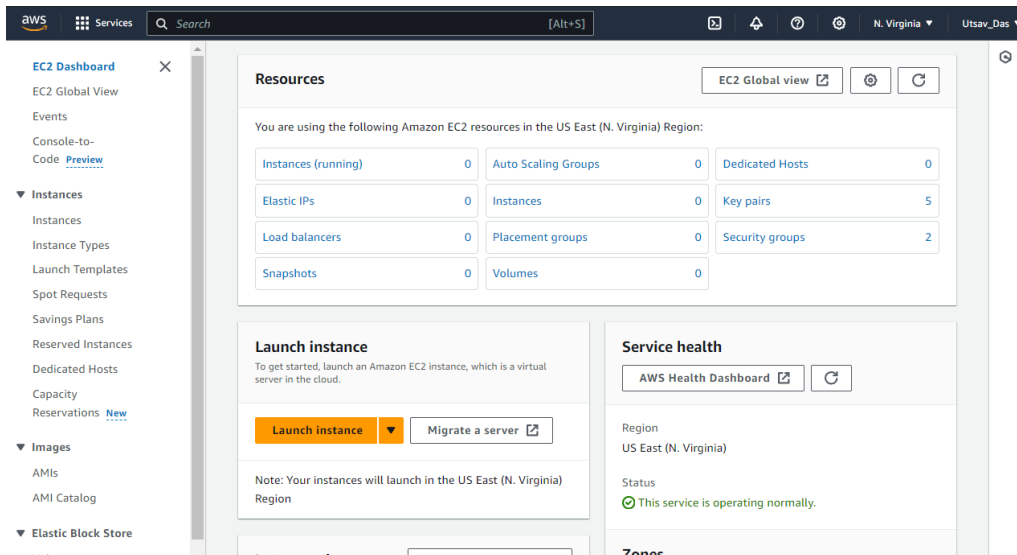


# Assignment – 10

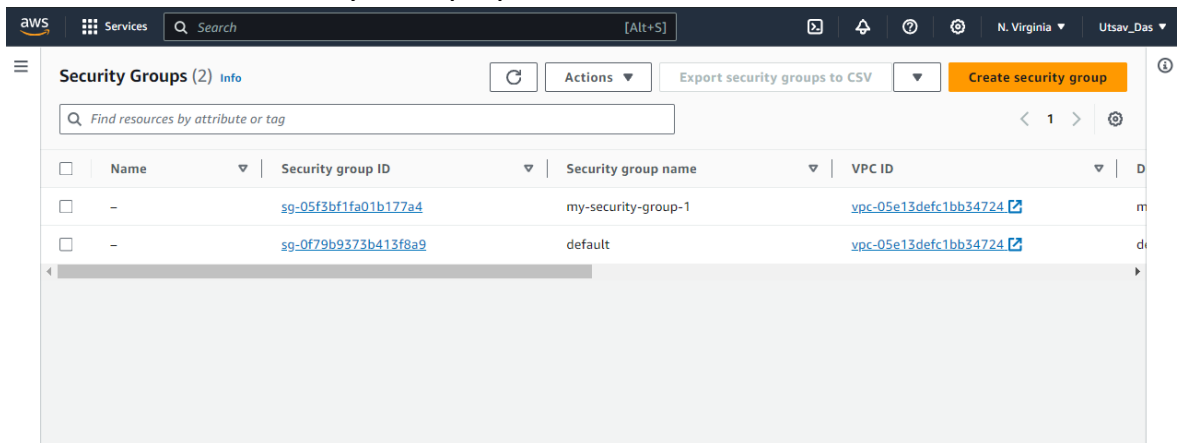
## Problem Statement:

Deploy a project from GitHub to EC2 by creating a new security group and user data.

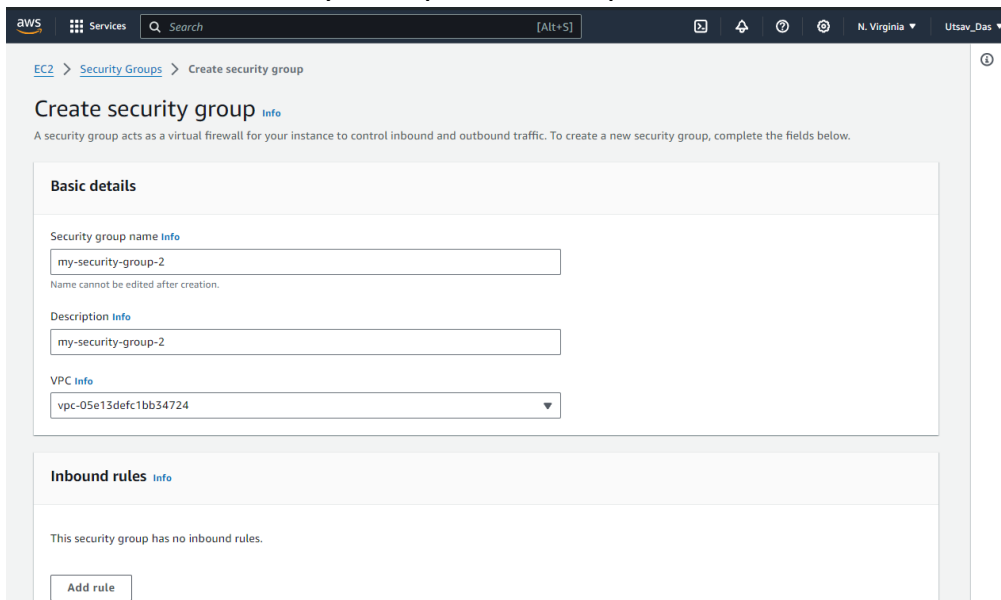
- 1) Go to EC2 and then to Security groups.



- 2) Click on Create Security Group option.



- 3) Give name of Security Group and description.



- 4) In Inbound rules click on Add rule. Here, we add all 4 rules: Custom TCP, SSH, HTTP, HTTPS and in Source select 0.0.0.0/0  
In port range of Custom TCP give 4000. Rest have default port number.

**Inbound rules** Info

Type	Protocol	Port range	Source	Description - optional	
Custom TCP	TCP	4000	Any... 0.0.0.0/0		Delete
SSH	TCP	22	Any... 0.0.0.0/0		Delete
HTTP	TCP	80	Any... 0.0.0.0/0		Delete
HTTPS	TCP	443	Any... 0.0.0.0/0		Delete

Add rule

- 5) Click on Create security group.

**Outbound rules** Info

Type	Protocol	Port range	Destination	Description - optional	
All traffic	All	All	C... 0.0.0.0/0		Delete

Add rule

Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag  
You can add up to 50 more tags

Cancel Create security group

- 6) Go back to instance and click on Launch instance.

**Resources** EC2 Global view

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	5
Load balancers	0	Placement groups	0	Security groups	3
Snapshots	0	Volumes	0		

**Launch instance**  
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance Migrate a server

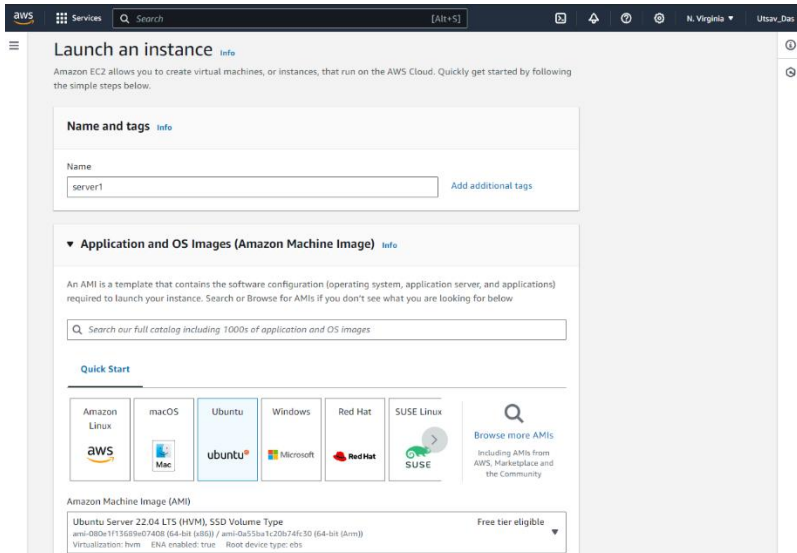
Note: Your instances will launch in the US East (N. Virginia) Region

**Service health**  
AWS Health Dashboard

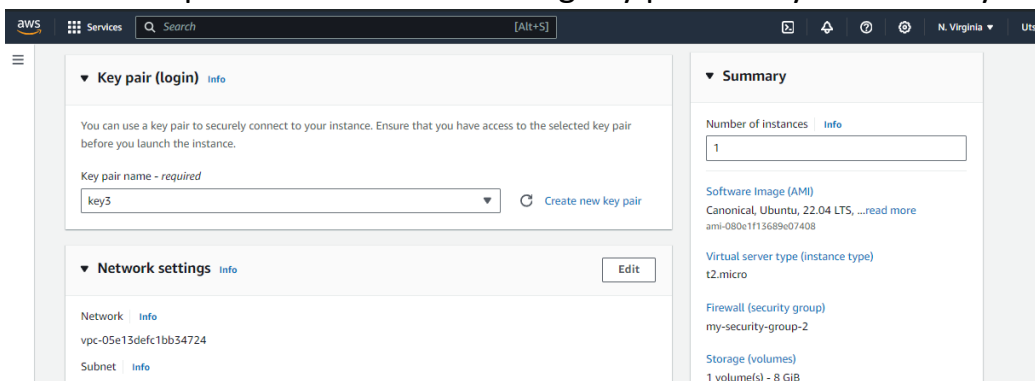
Region  
US East (N. Virginia)

Status  
This service is operating normally.

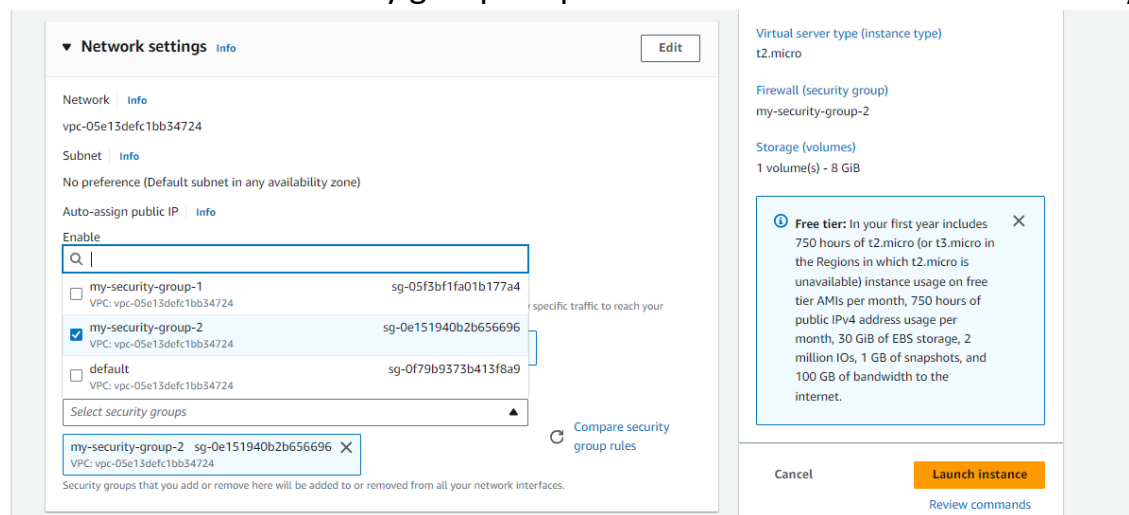
7) Give name of instance and in Application and OS Images select Ubuntu.



8) Click on dropdown and select existing key pair as key was already created before.



9) Click on Common Security group dropdown and select the created security group.

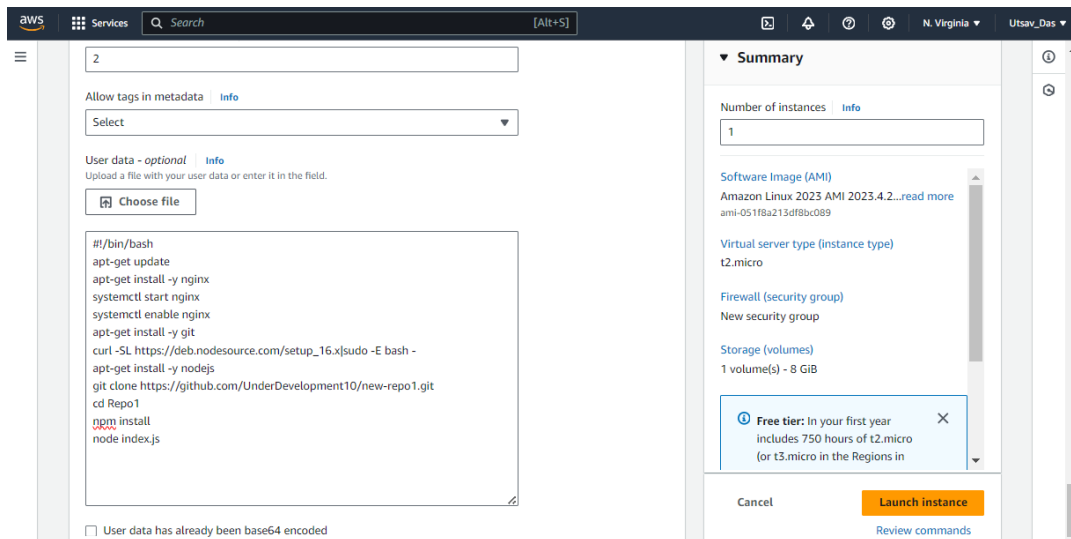


10) Go to advanced detailed section and then expand it and then go to User data section and write these commands:

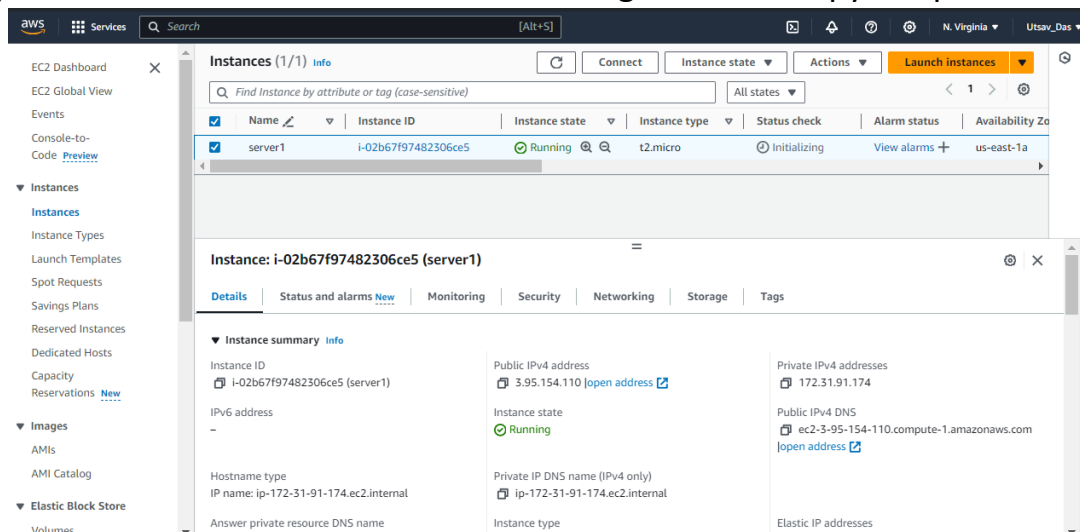
- `#!/bin/bash`
- `apt-get update`
- `apt-get install -y nginx`
- `systemctl start nginx`
- `systemctl enable nginx`
- `apt-get install -y git`

- `curl -SL https://deb.nodesource.com/setup_16.x|sudo -E bash -`
- `apt-get install -y nodejs`
- `git clone https://github.com/UnderDevelopment10/new-repo1.git`
- `cd repo2`
- `npm install`
- `node index.js`

After it click on Launch instance.



11) Go back to Instances and click on running instance. Copy the public IPv4 address.



12) Paste it in another tab and enter port no. 4000 at end of URL.

