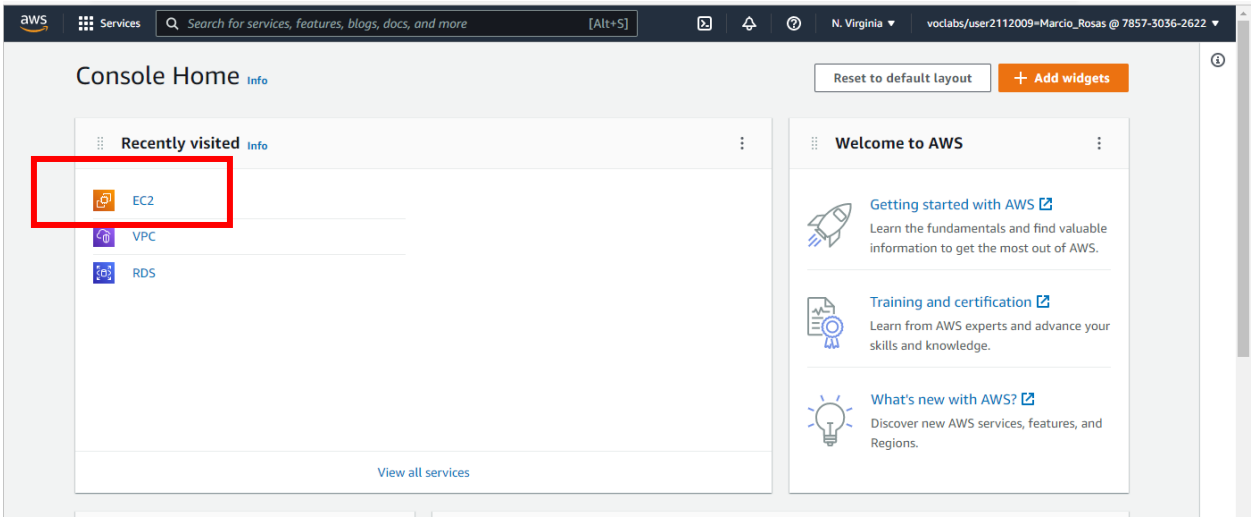
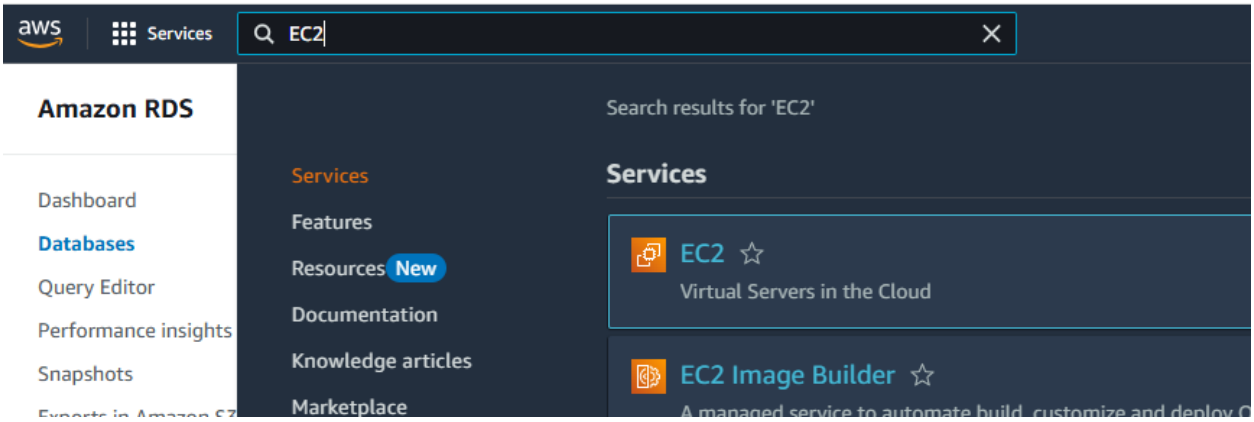
Creating EC2 Instance on AWS: Instructions

Go to AWS Academy (https://awsacademy.instructure.com/), start your lab and go the AWS console Home. Revisit the instruction for RDS setup if you need (they are in Canvas, files/Create DB file)

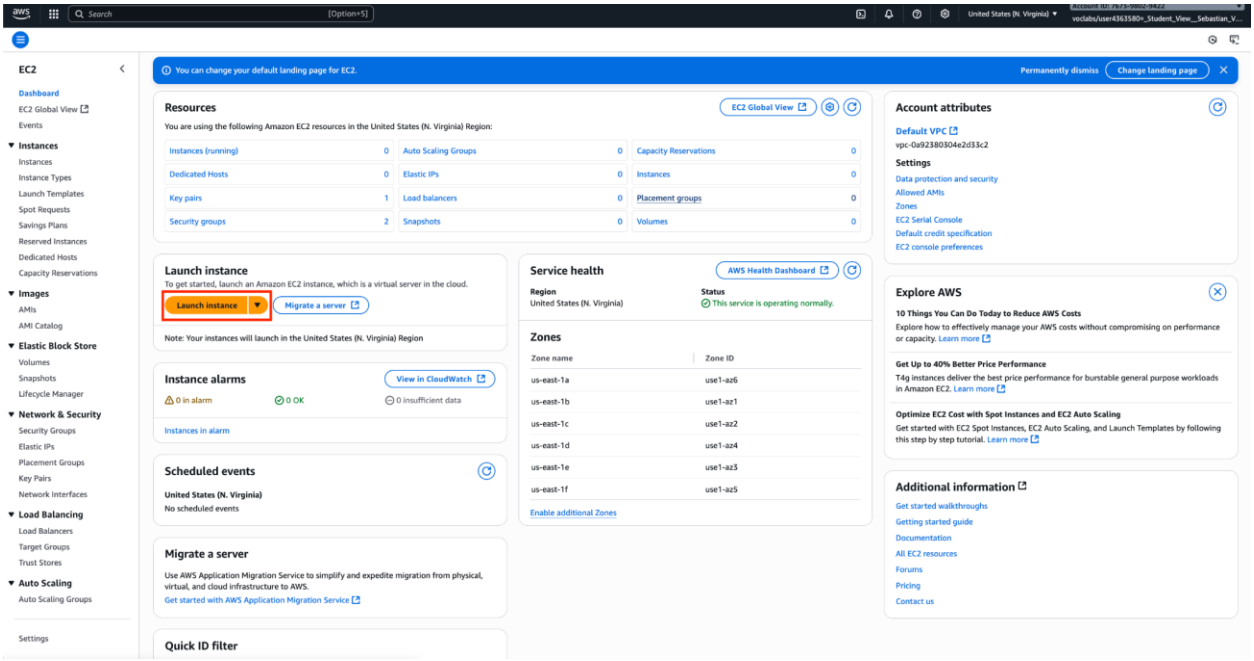
On the Console Home, click on EC2:



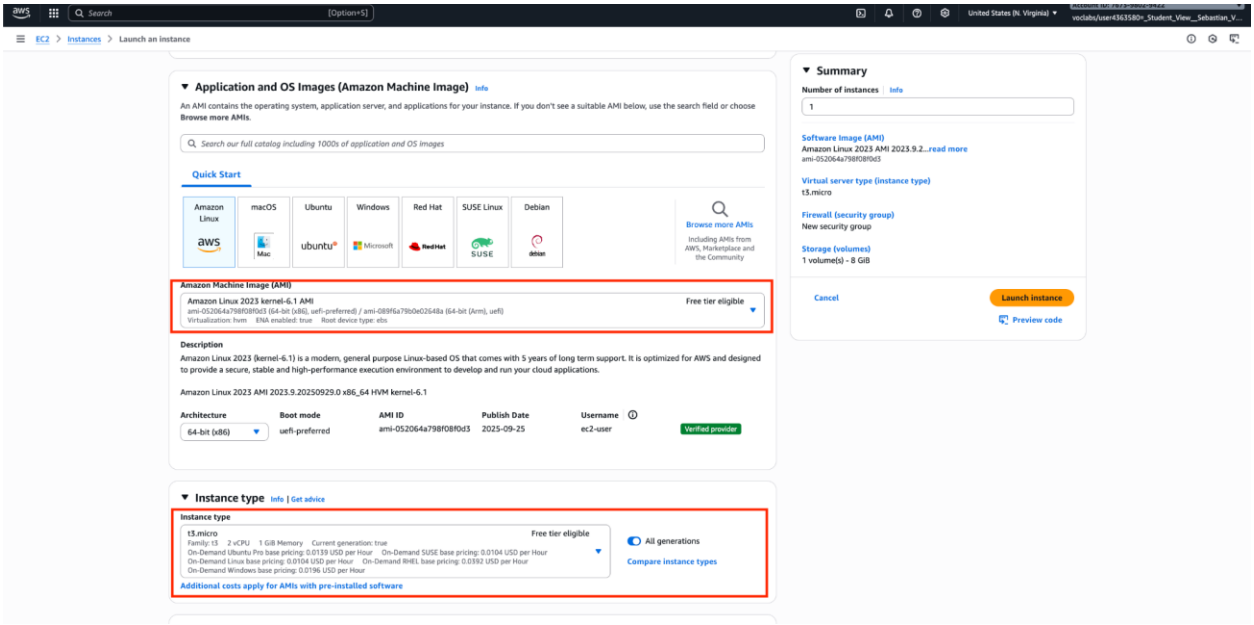
Or simply type EC2 o the search bar:



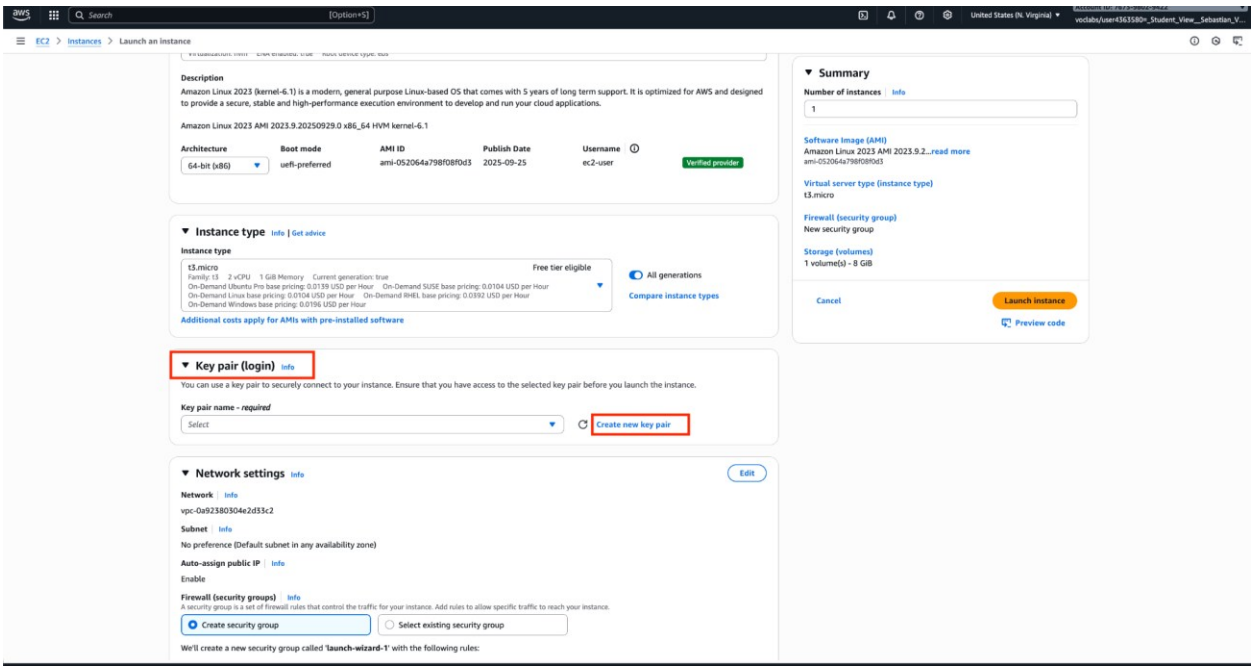
From the console dashboard, choose Launch Instance



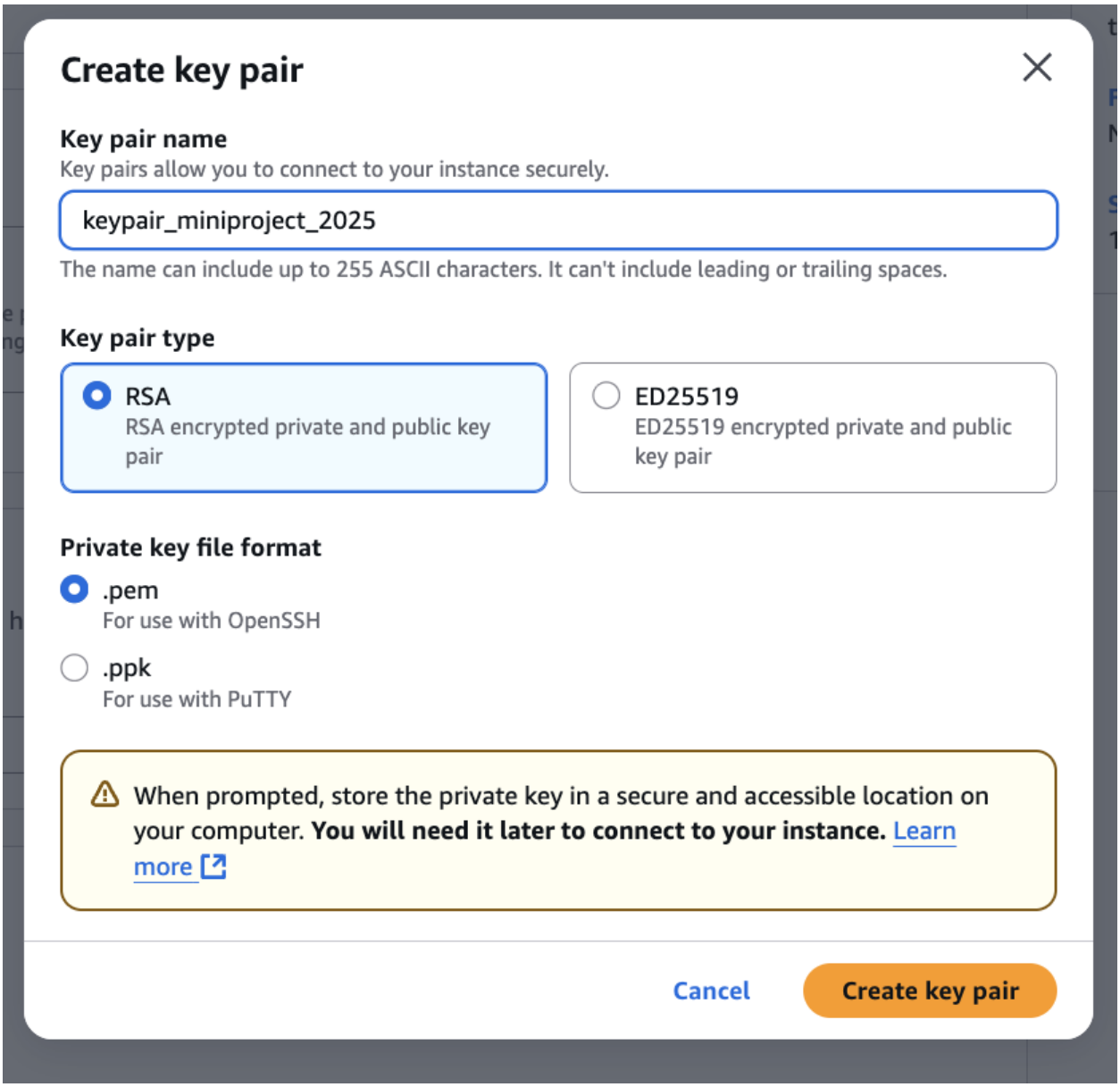
In the next screen, choose:



Scroll down to the section “Key Pair(login)” and click on “create New Key pair”, as highlighted below:

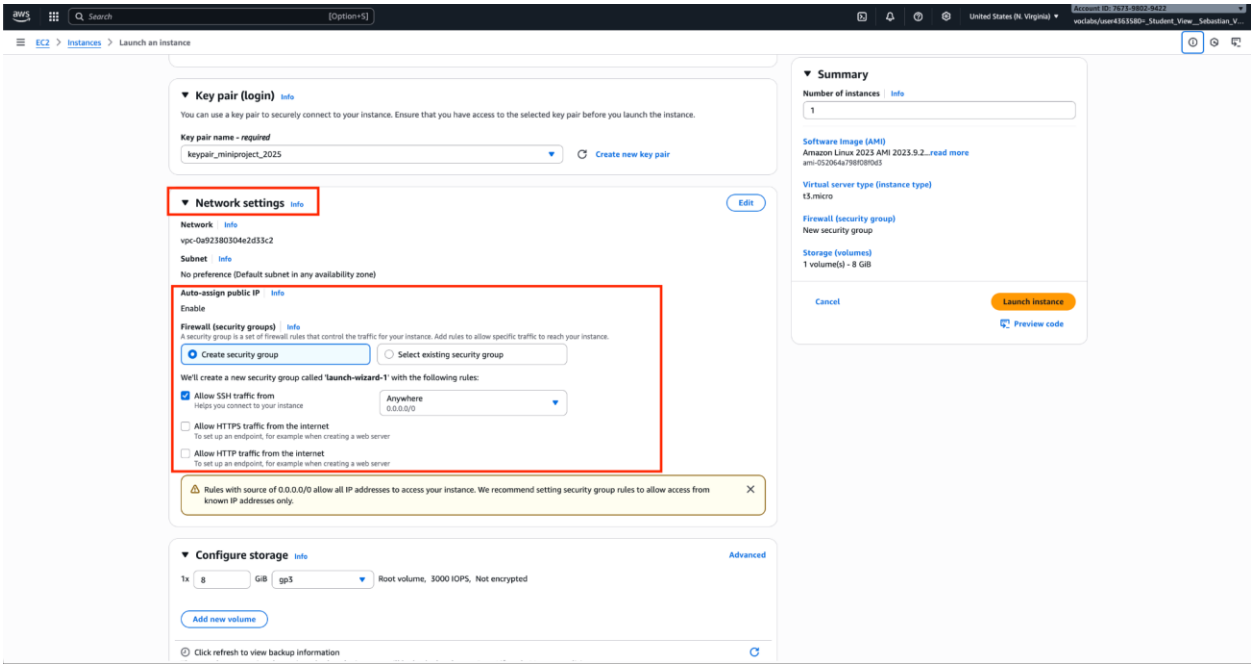


You will see the screen below. Give a meaningful name to your new key pair and click on the orange button “Create key pair”.

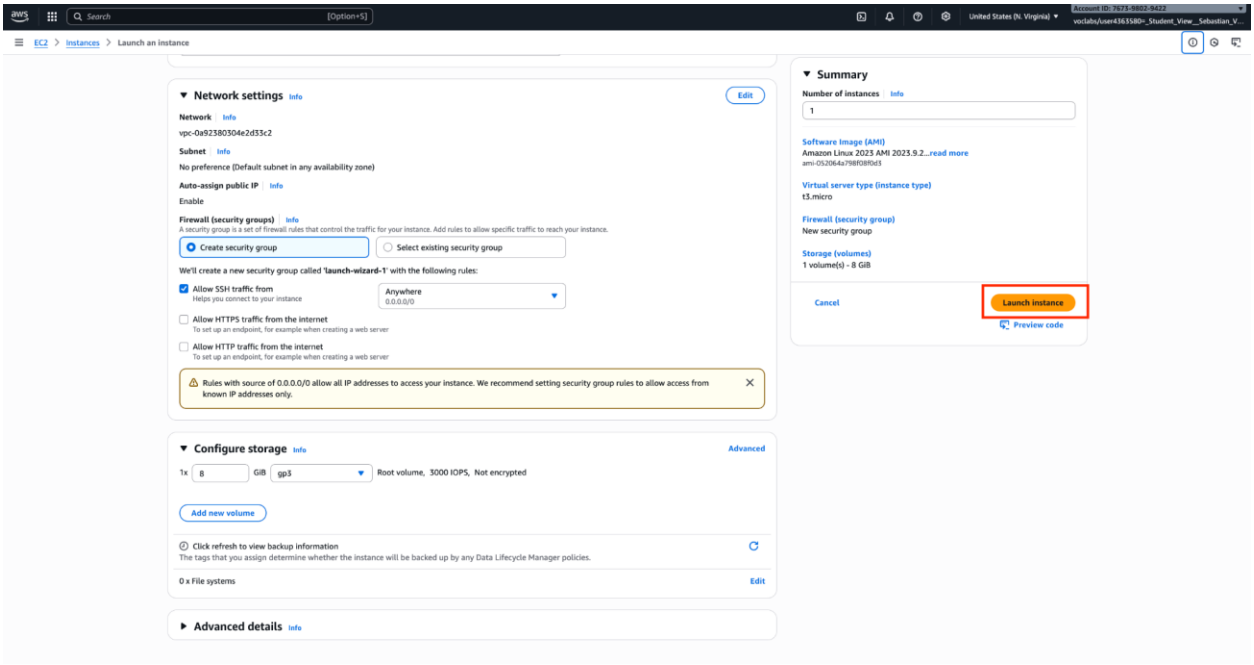


This will download a .pem file to your computer. Move this pen file to the ssh folder of your computer (usually, this folder is directly under your user in your file system). **Make sure you remember this folder location and this file name. You will need them later on, to connect to your EC2.**

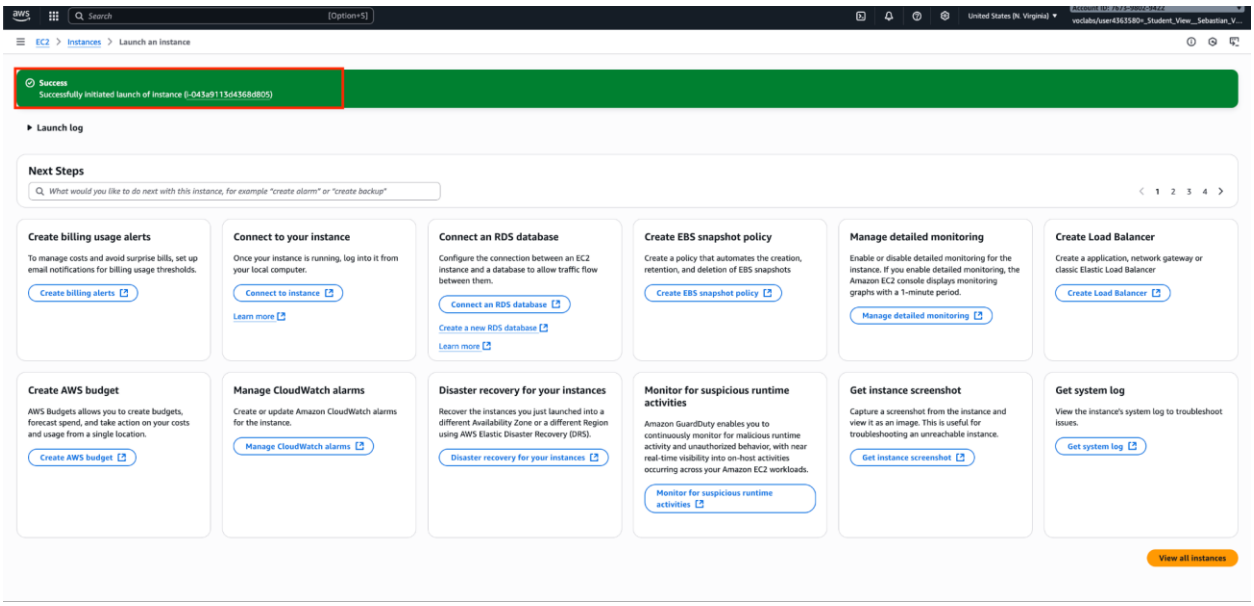
Scroll down to the network settings section and make sure that your settings are like the highlighted areas below:


Search
[Option+S]
United States (N. Virginia)
EC2 > Instances > Launch an instance
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
keypair_miniproject_2025
Create new key pair
Network settings Info
Edit
Network Info
vpc-0a92380304e2d33c2
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-1' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage Info
Advanced
1x
8
GiB
gp3
Root volume, 3000 IOPS, Not encrypted
Add new volume
Click refresh to view backup information
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code

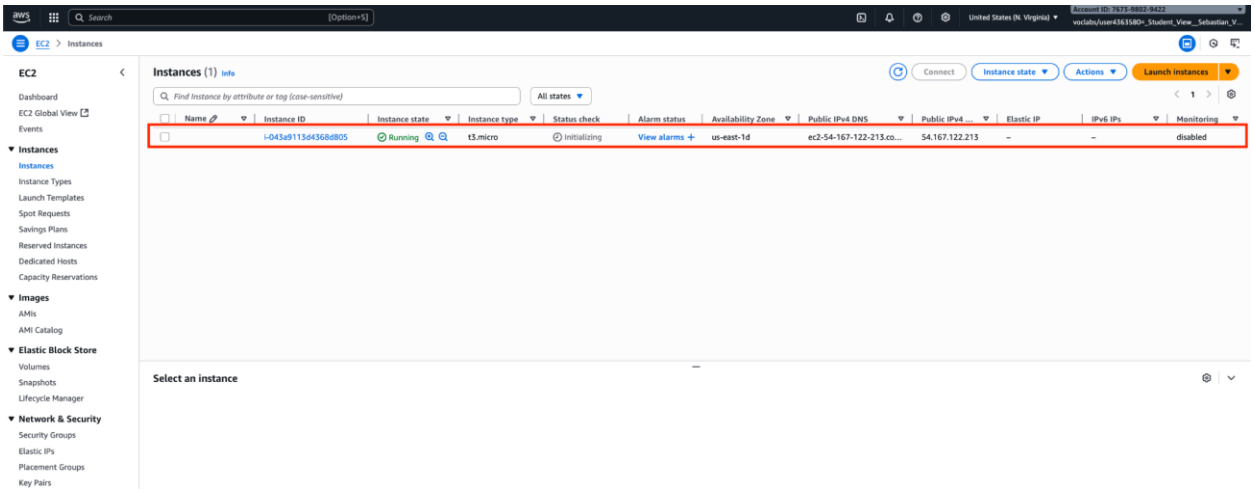
After that, click “launch instance” using the orange button on the right section of the screen:



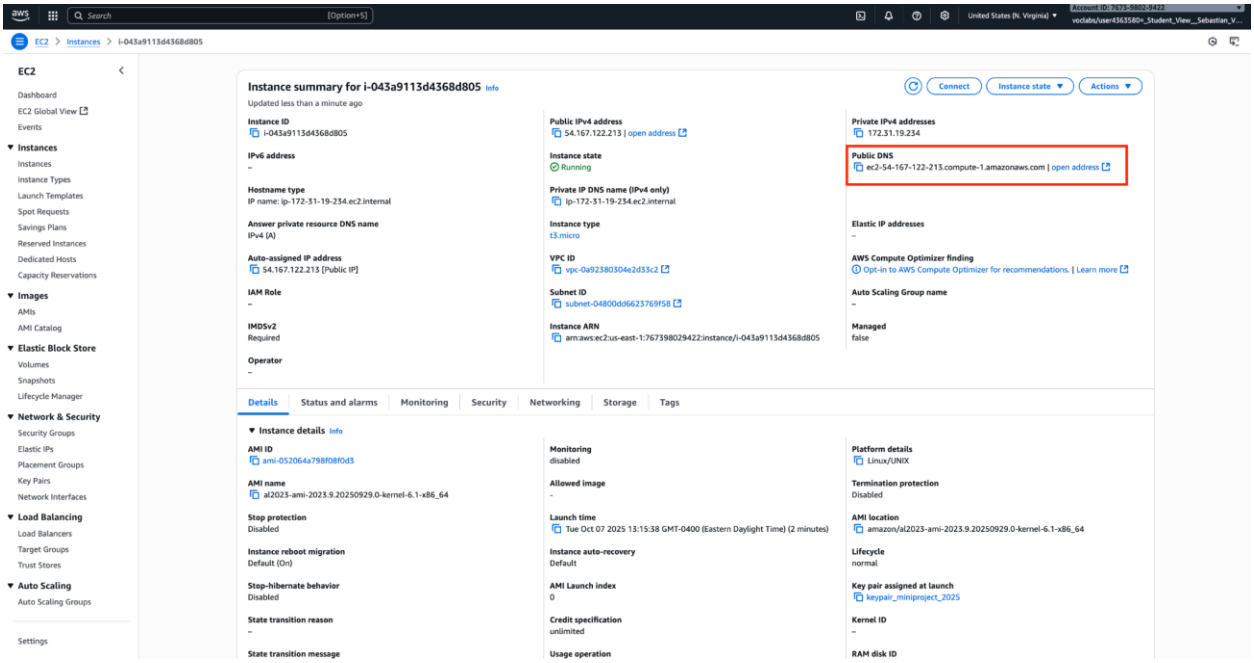
You will see this screen below, confirming your EC2 instance has been correctly launched. Click on the highlighted area to navigate to your EC2 dashboard.



On the Ec2 dashboard, you'll see the screen below. Click on the highlighted area to open your ec2 details.



You'll see the screen below with all the details of your EC2. Copy the public IPv4 DNS (yours will be different from the one in the screen below). You'll need to paste it on your terminal (Power Shell or Terminal) to connect with your EC2 from your computer.



Now, open your Mac OS Terminal or Windows Power shell and type:

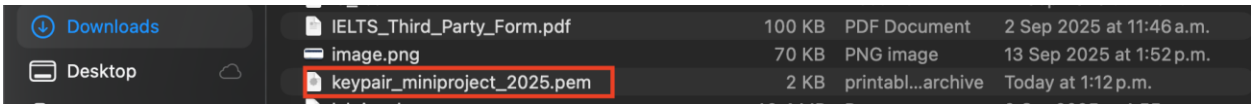
- keep in mind that, regarding **ssh/your_keypair_name.pem** and **your_public_IPv4**:

- **ssh** is the folder where you put the key pair you created. If you put it into a different folder, you need to use the correct path to the file here. (it may be .ssh in your computer)
- **your_keypair_name.pem** refers to the name you gave to your key pair. Yours should be different than this.
- **your_public_IPv4** is the one you copied from AWS

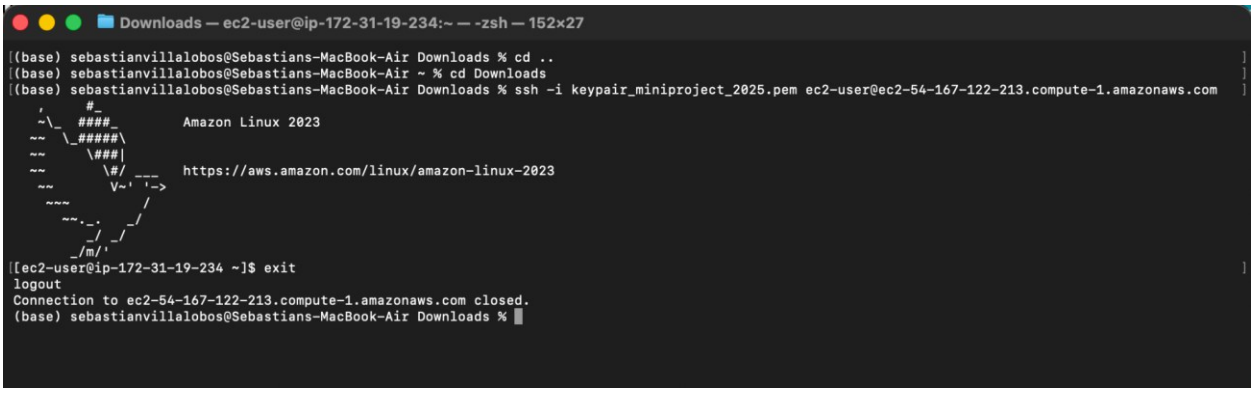
Command: ssh -i “path_to_your_file”/your_keypair_name.pem ec2-user@your_public_IPv4

MAC

- My .pem file is located in the Downloads folder

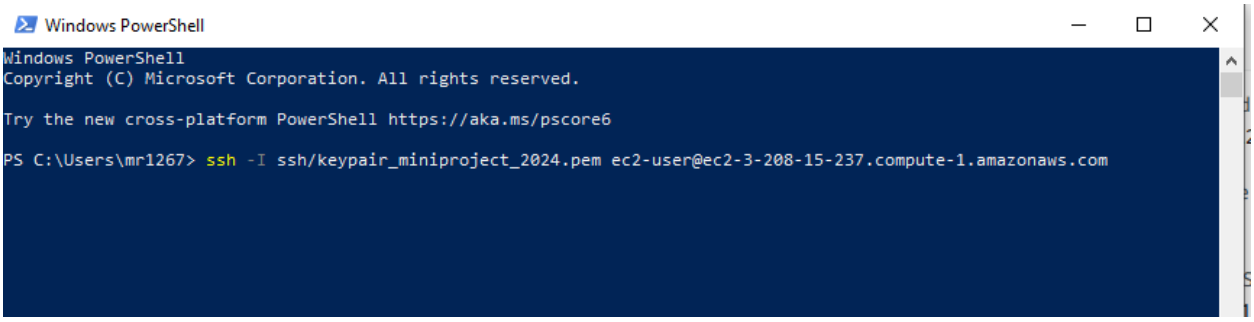


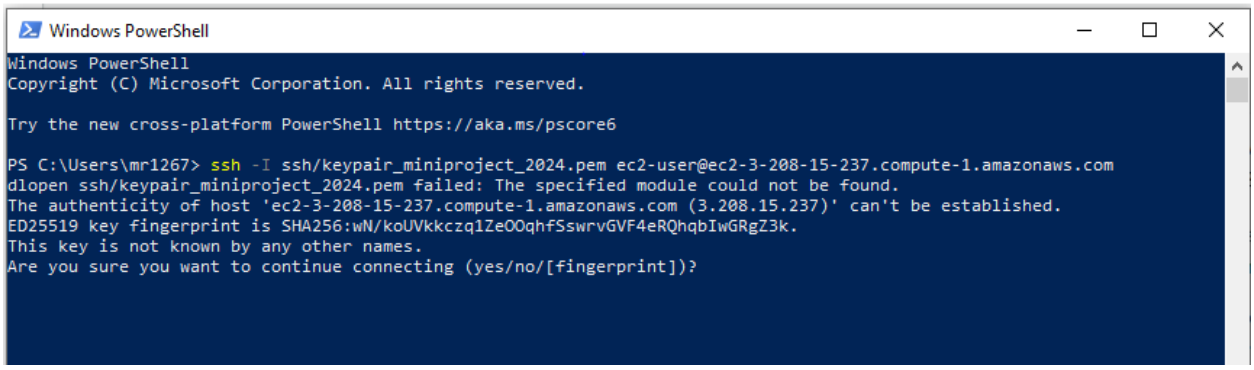
- You may need to change the permissions of the .pem folder, to do this you just need to run the following command - chmod 400 “path_to_your_file”/your_keypair_name.pem



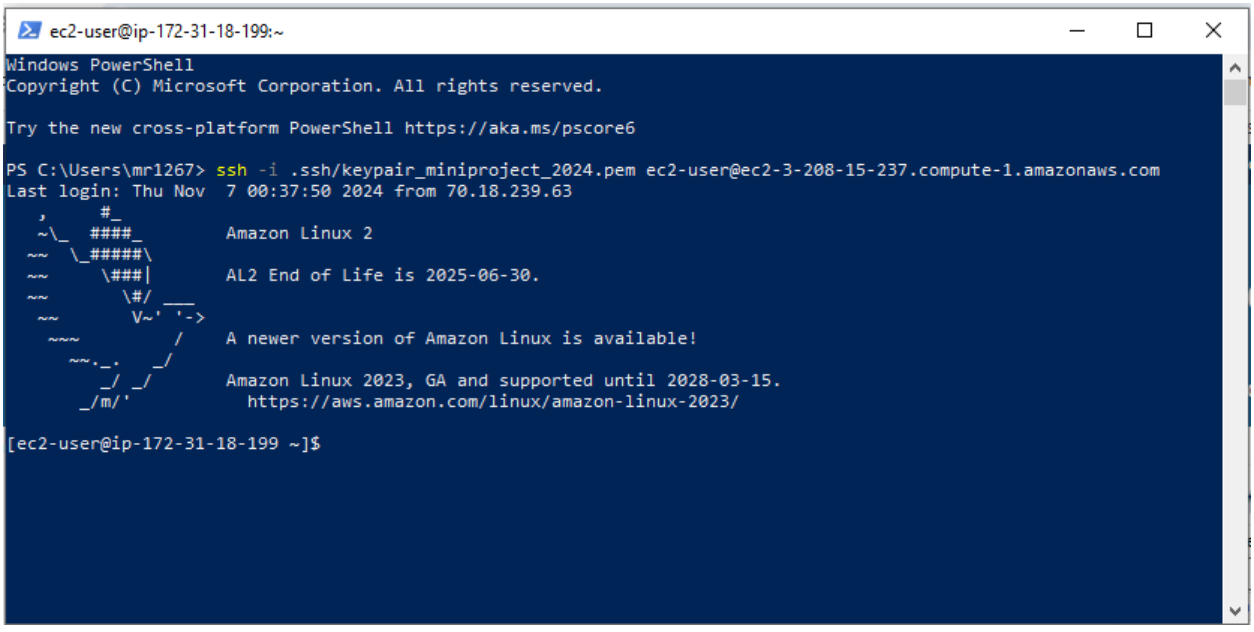
WINDOWS

Your terminal screen should look like this:

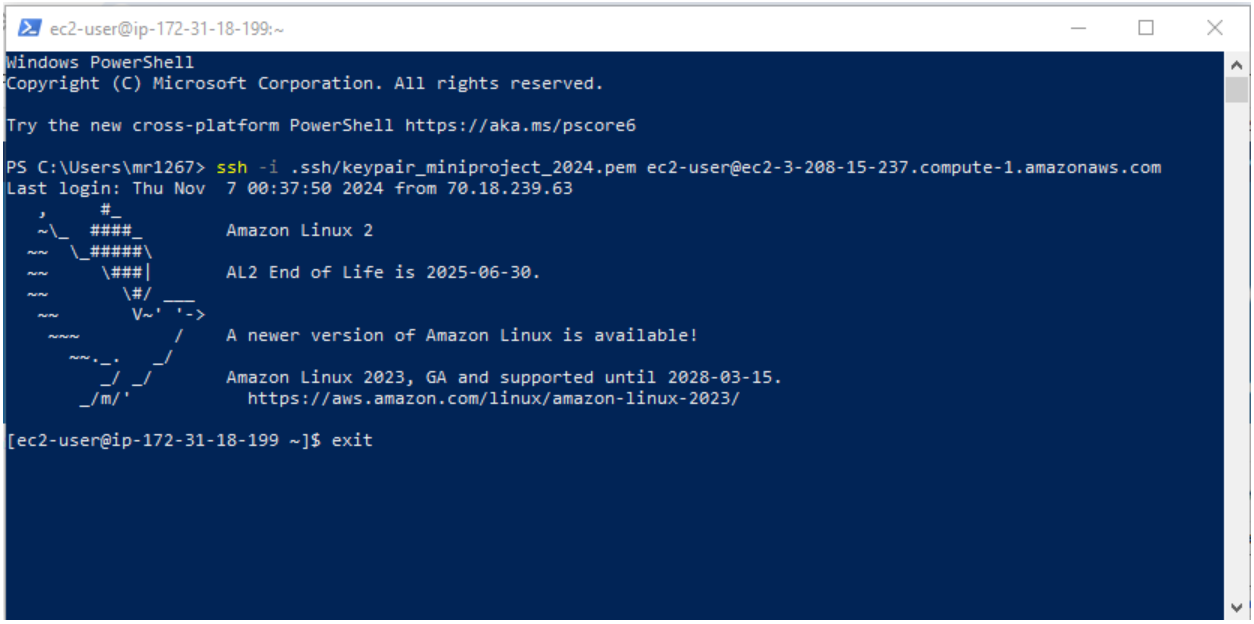




After you hit enter, you should see the following, confirming that you have successfully connected to your EC2.



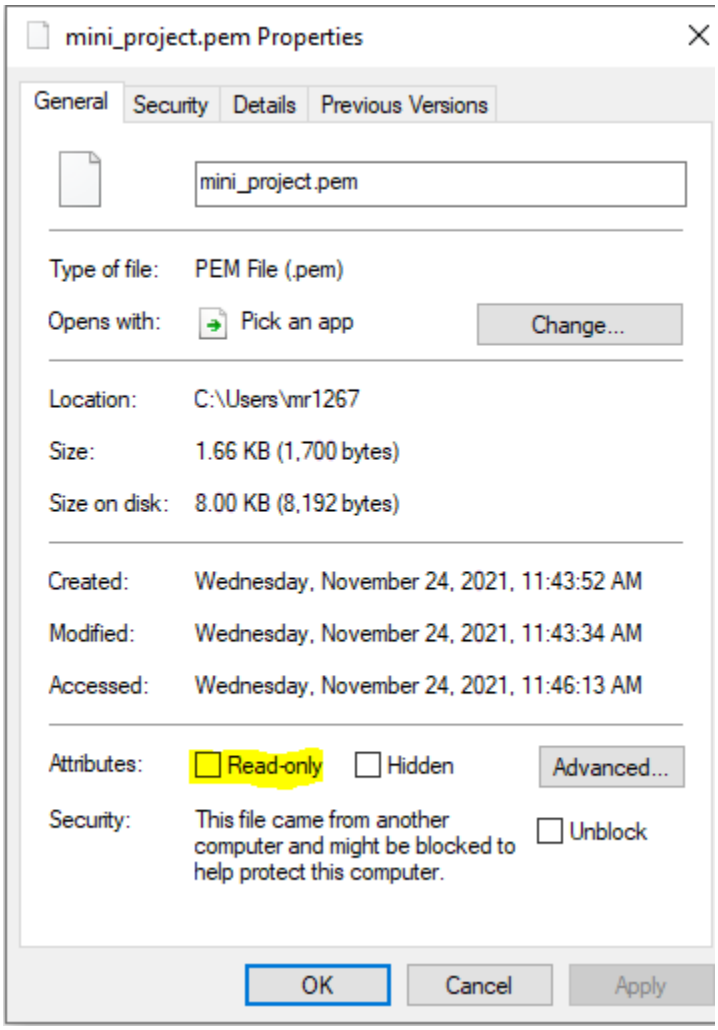
Once you see this screen, logout from the EC2 by typing “exit” with go back from the Ec2 to your computer (terminal or Power Shell) and then return to the to the Mini-project Instructions.


ec2-user@ip-172-31-18-199:~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\mr1267> ssh -i .ssh/keypair_miniproject_2024.pem ec2-user@ec2-3-208-15-237.compute-1.amazonaws.com
Last login: Thu Nov 7 00:37:50 2024 from 70.18.239.63
Amazon Linux 2
AL2 End of Life is 2025-06-30.
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-172-31-18-199 ~]$ exit

Troubleshooting:

Windows users:

You may need to change the permissions of your_keypair.pem file to ready only. You can do that manually via Windows by right clicking on it and making the change in the screen below::



Mac users:

Permissions to your_keypair.pem filemust be set to read-only by owner. For that, use the command chmod 400 your_key_file.pem on your terminal.

NOTE: if more than one person uses your computer, the .pem file have have inherited permissions for more then one user and this will result in your connection with the eC2 to be rejected.

If that happens to you, make sure to remove the inherited permissions to the .pem file and that only your current user has read only access to it.