Experiments on AWS EC2

University of Crete > CS 590.45 > Tutorial 2025

Efthimis Papageorgiou

Elastic Compute Cloud (EC2)

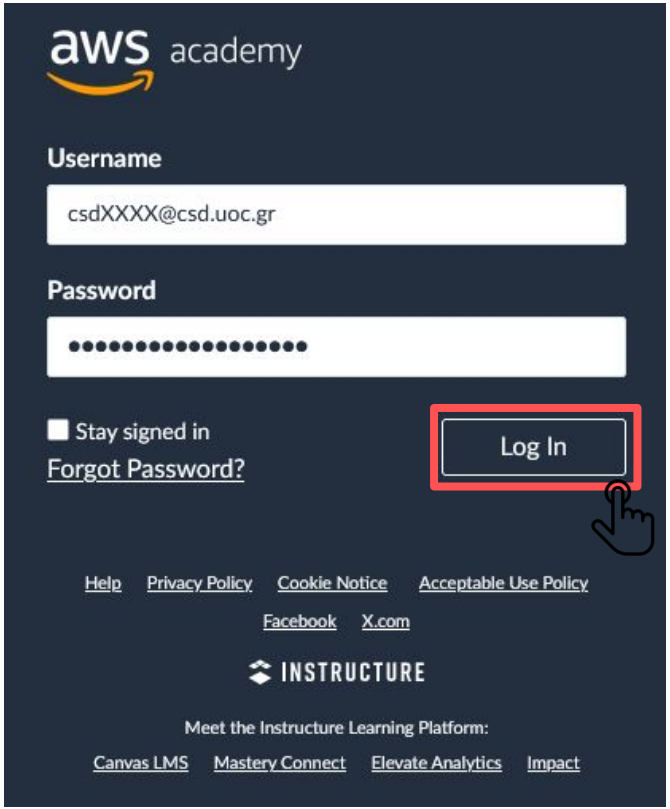
- What is EC2 ?
  - It's a **Virtual Machine** (VM) in the cloud
  - Provides on-demand computing power
  - Scales up or down as needed

- Features
  - **Pay-as-you-go Model** (pay for the hours a server runs)
  - Integrates with AWS services (e.g., connecting EC2 with S3 for storage or RDS for databases)
  - Various instance types (e.g compute-optimized for AI training)

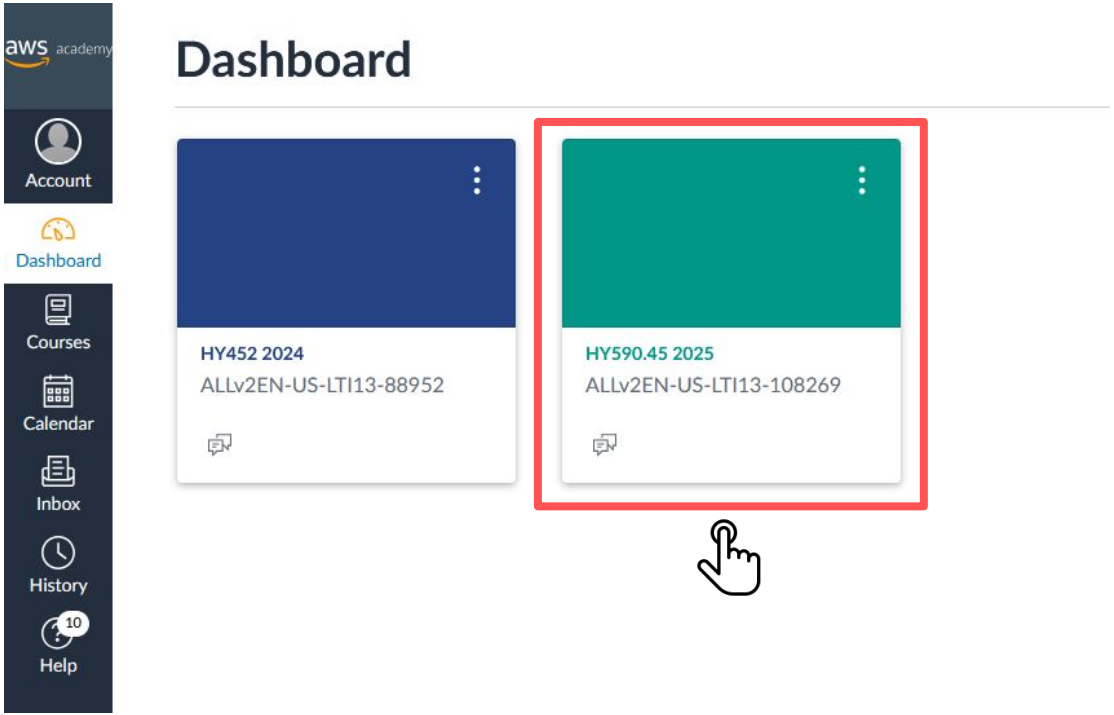
Login


aws academy
Student Login
(For students enrolled in a class)
学生の方はこちらからログインしてください。
已注册课程的学生请在这里登录
Educator Login
(For educators who have access to the AWS Academy Portal)
講師の方（AWS Academyメンバーポータルのアカウントをお持ちの方）はこちらからログインしてください。
教师请在这里登录（您需使用AWS Academy Portal账户登录）

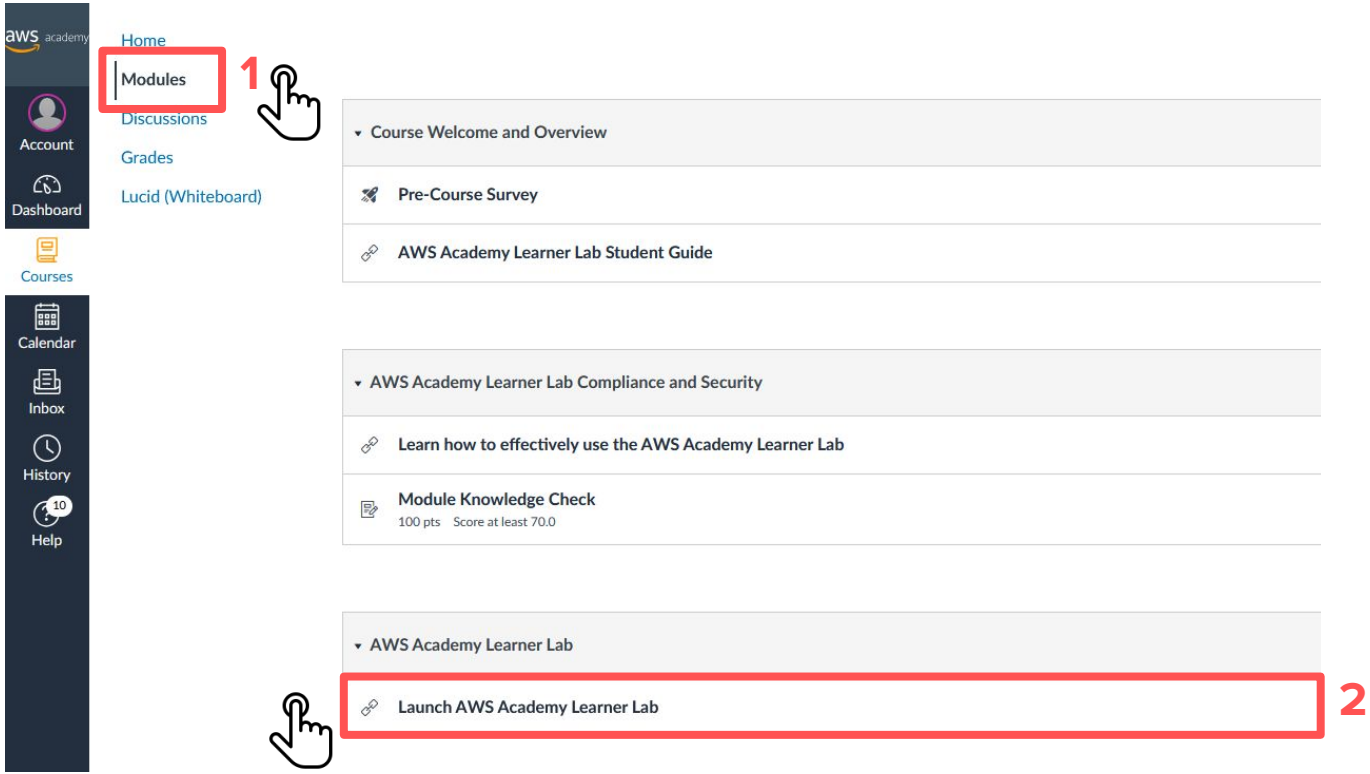
Username / Password



Select the course

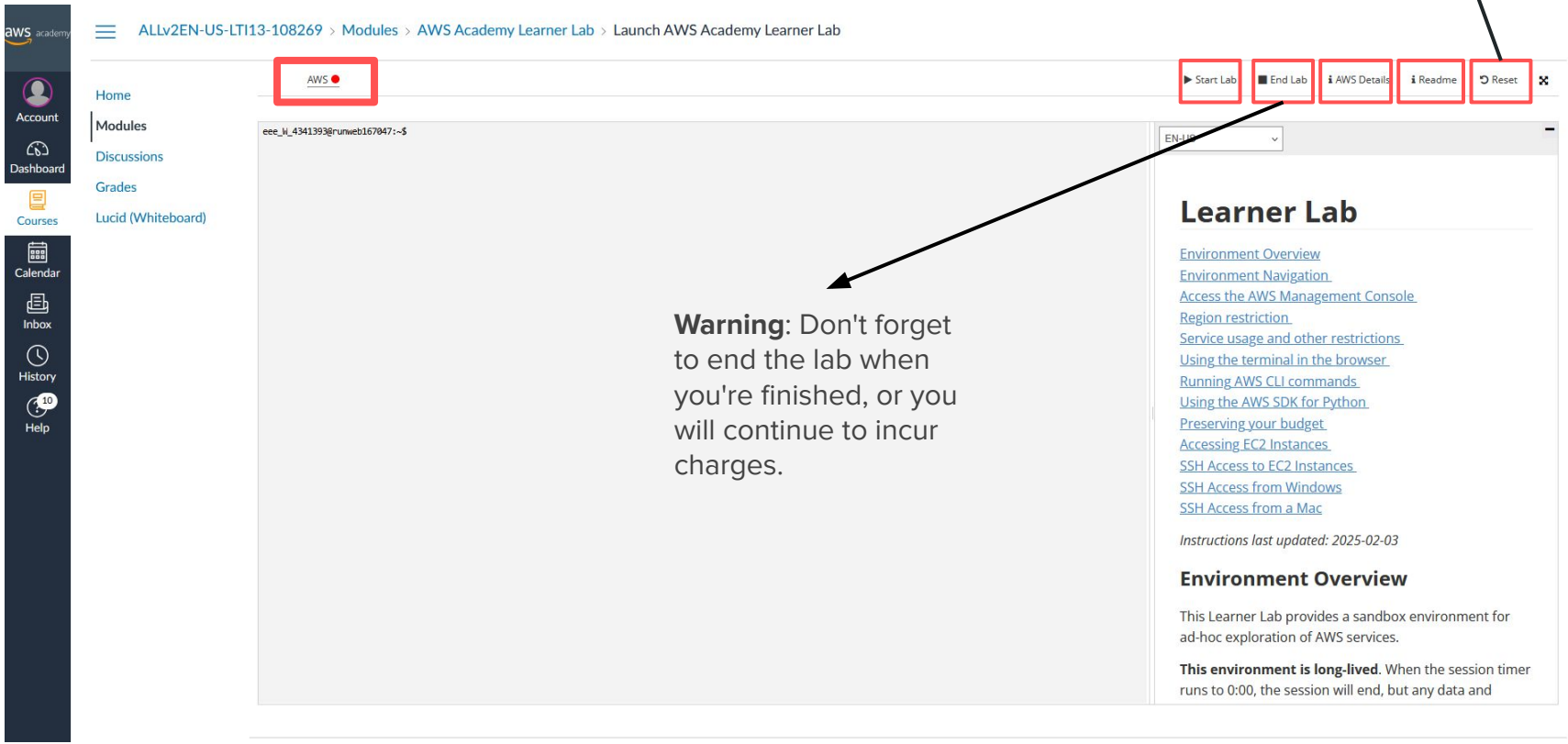


Launching Academy Learner Lab

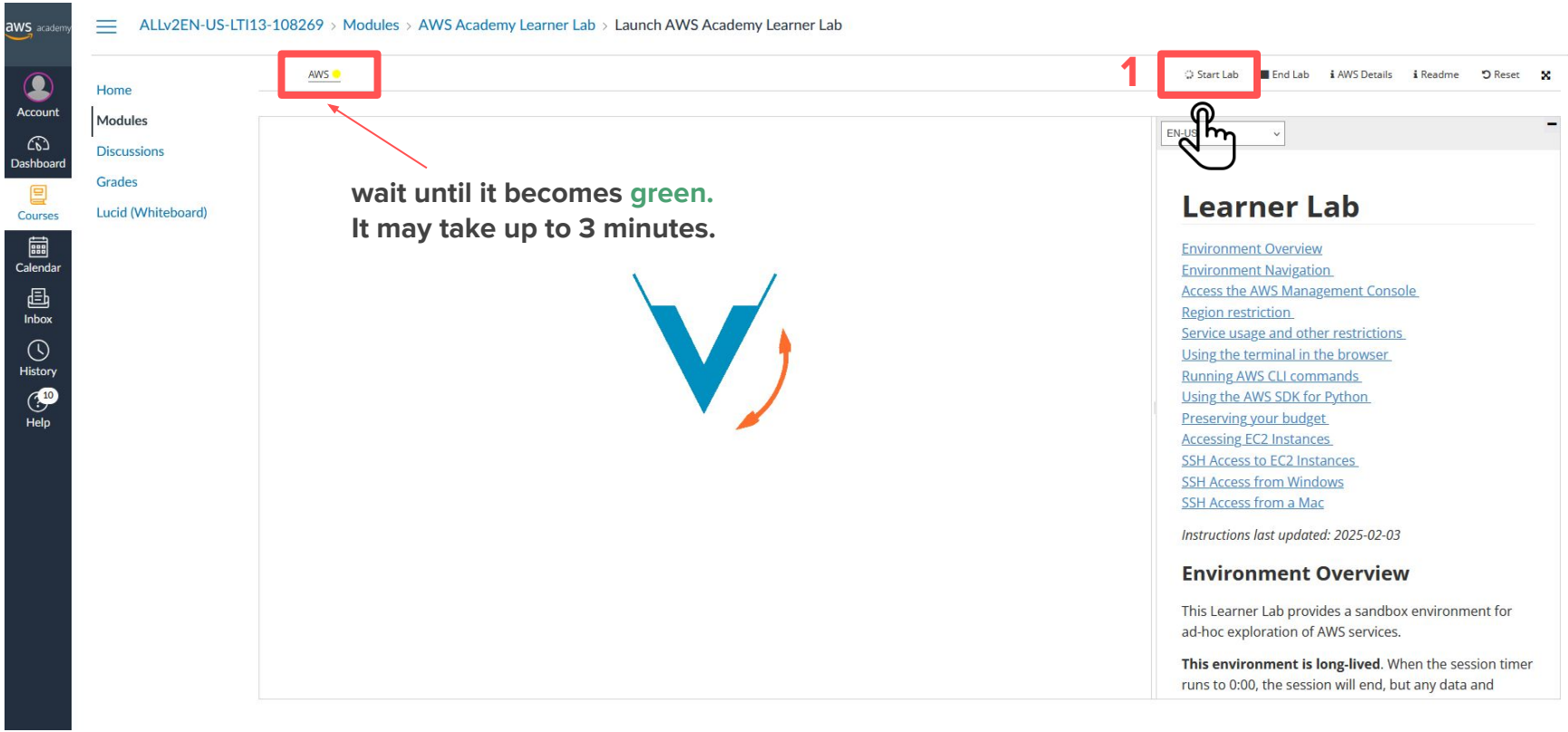


Environment Overview

Warning: Do not click this! Clicking it will delete everything you've done.

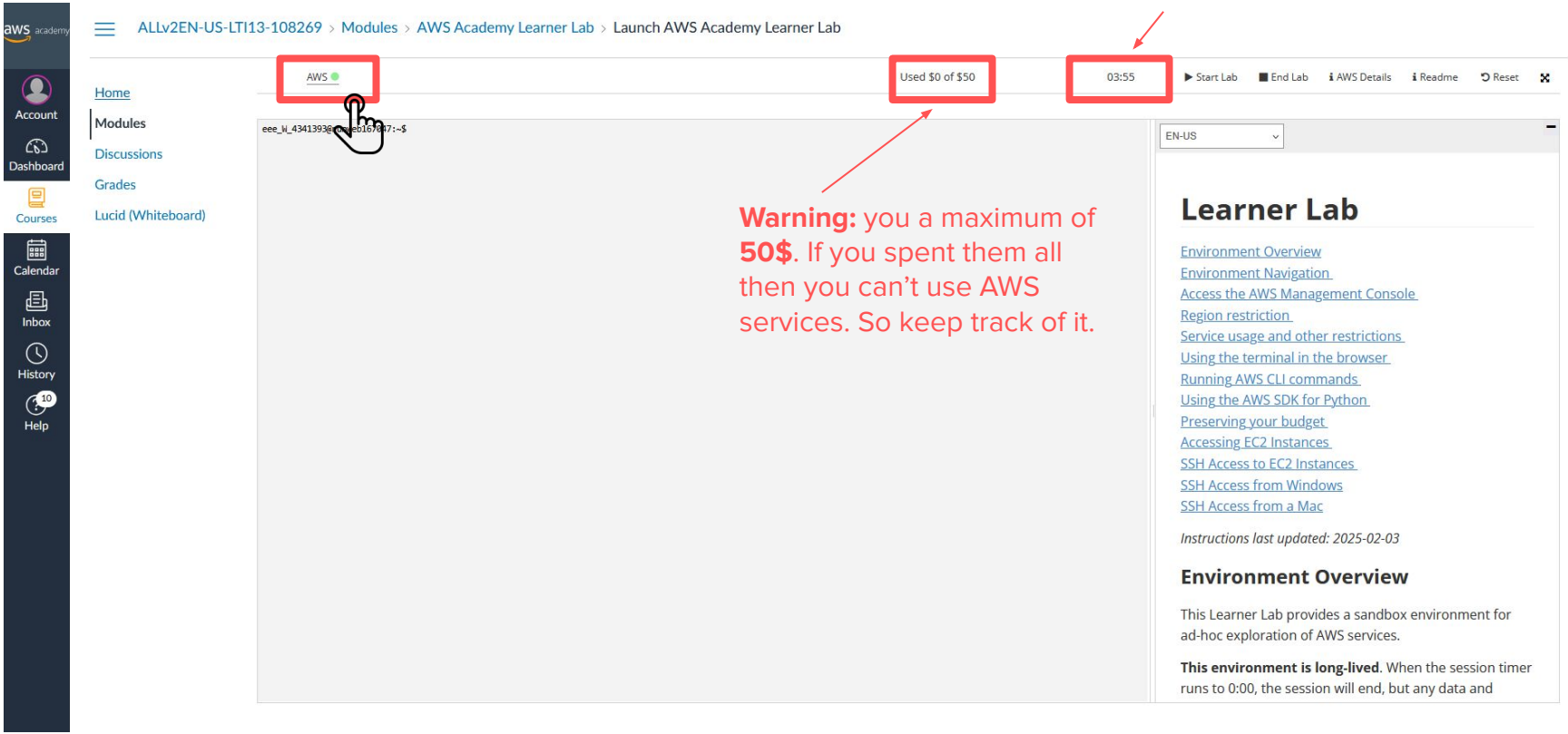


Starting the Lab



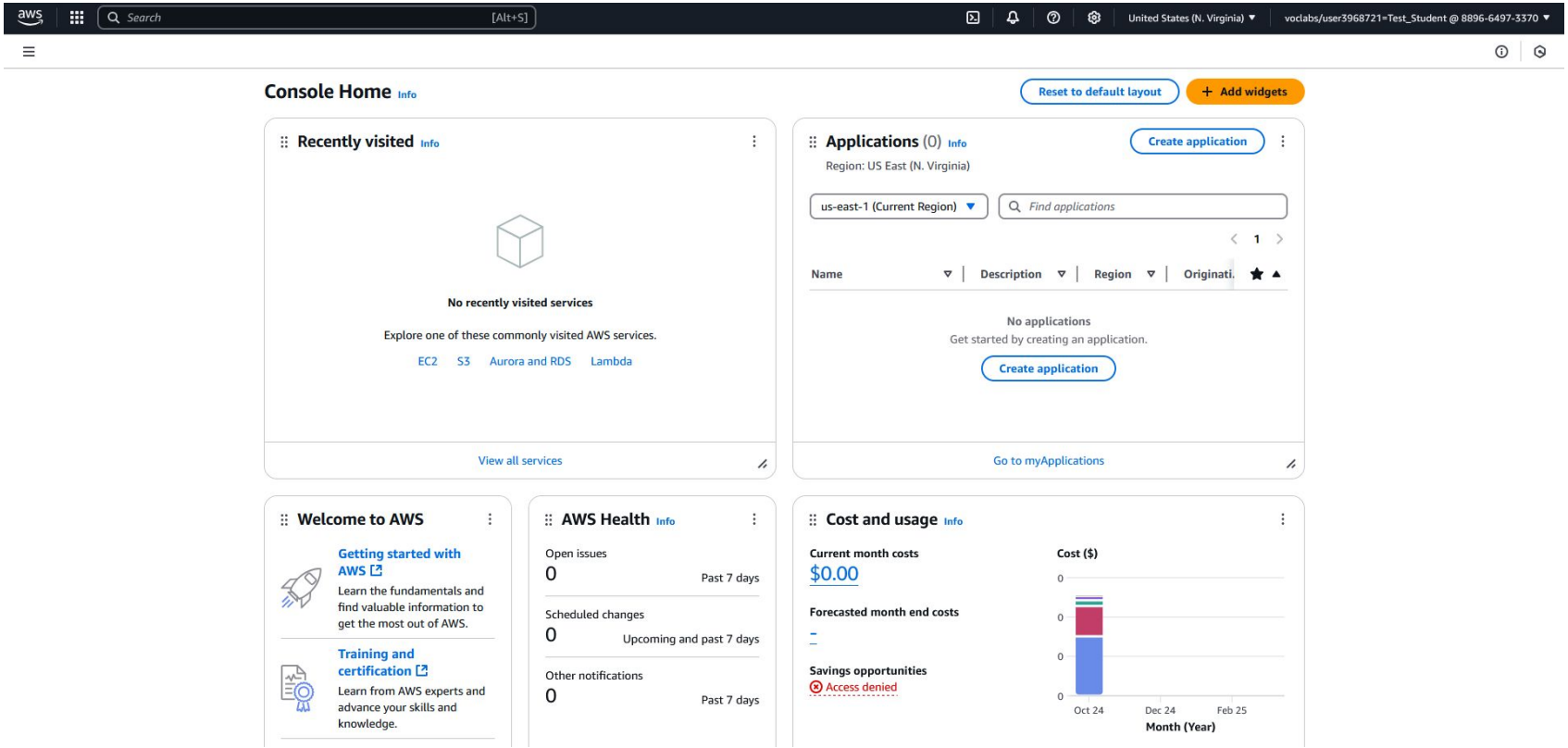
Entering the lab

every 4 hours, the lab session ends. Your don't lose any data

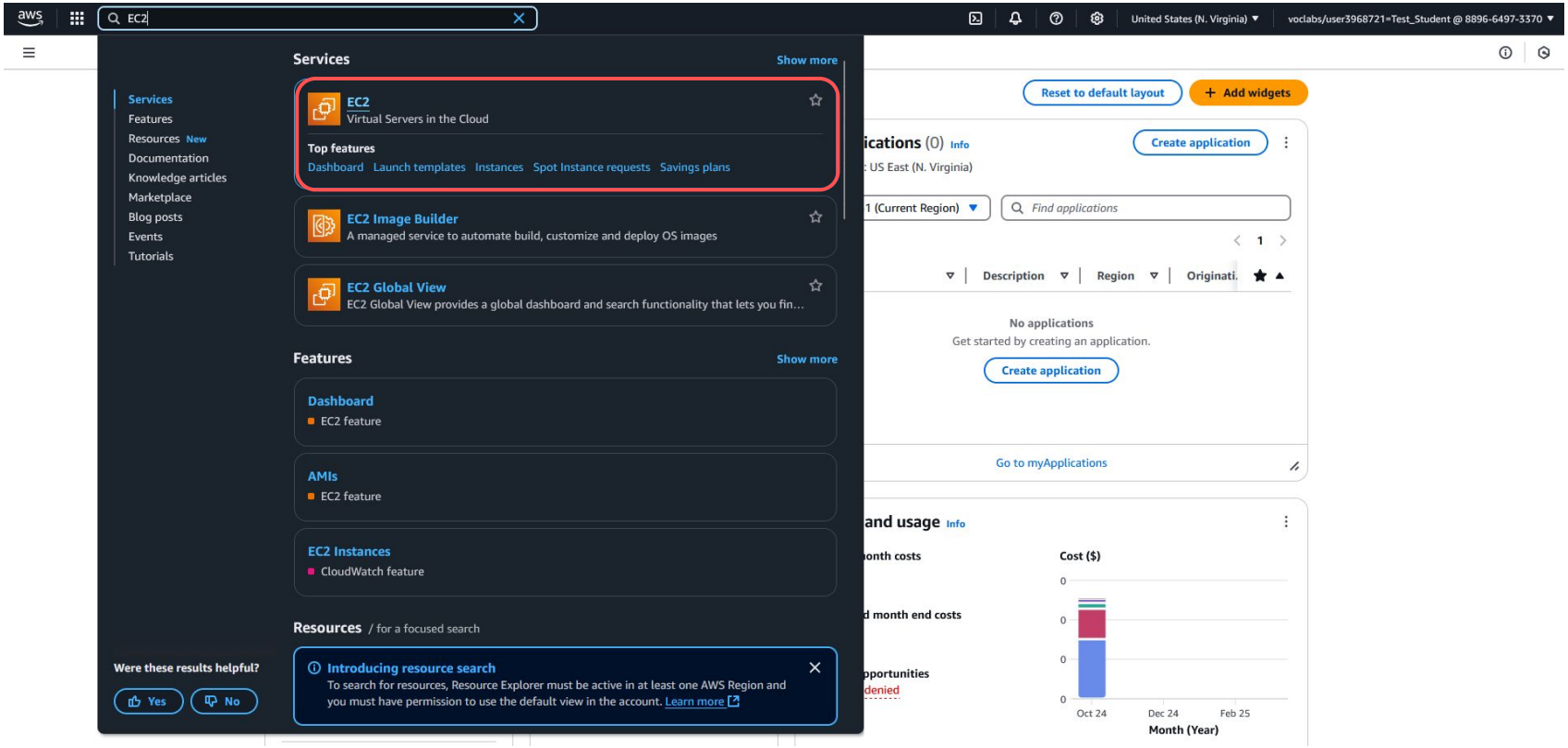


Warning: you a maximum of **50$**. If you spent them all then you can't use AWS services. So keep track of it.

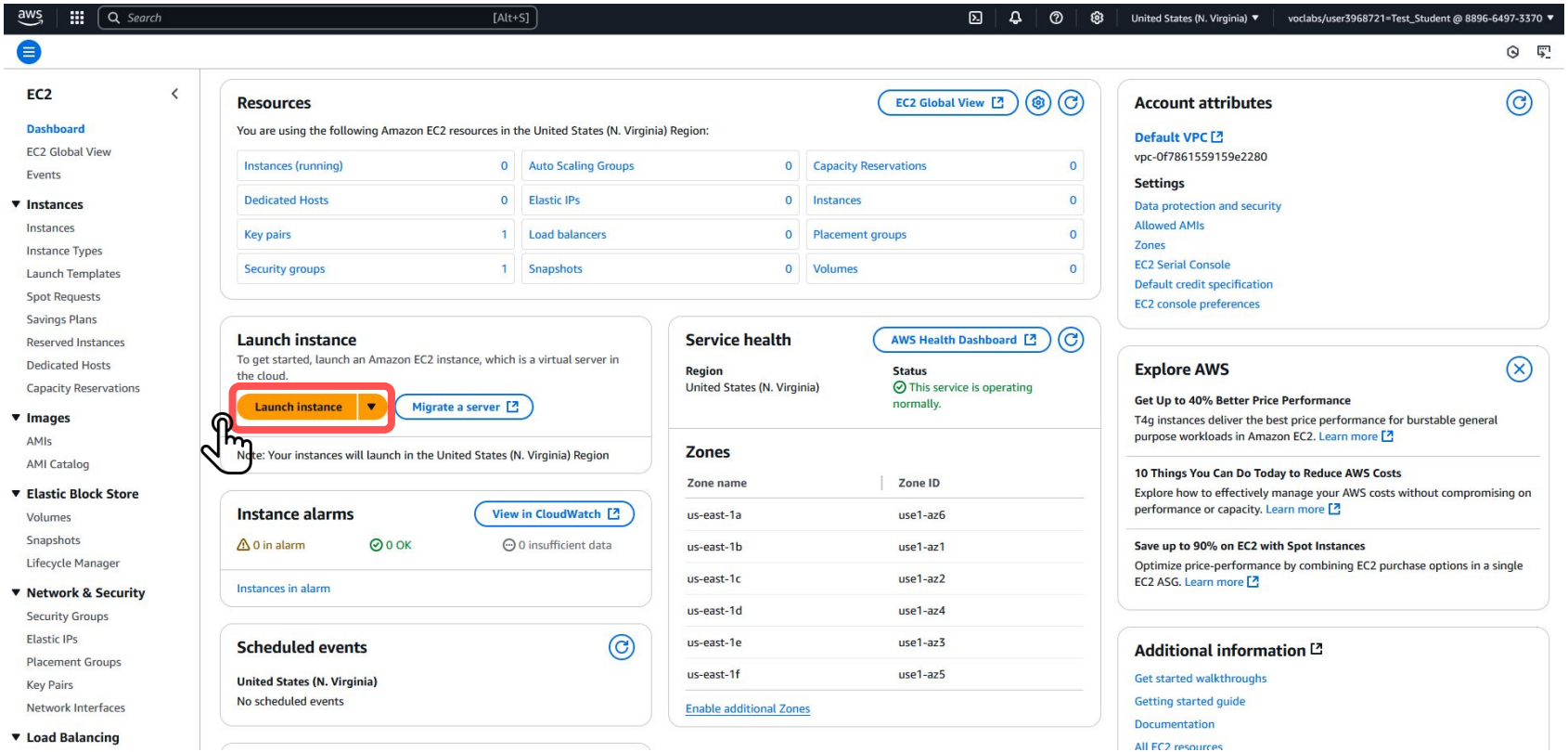
Welcome to AWS



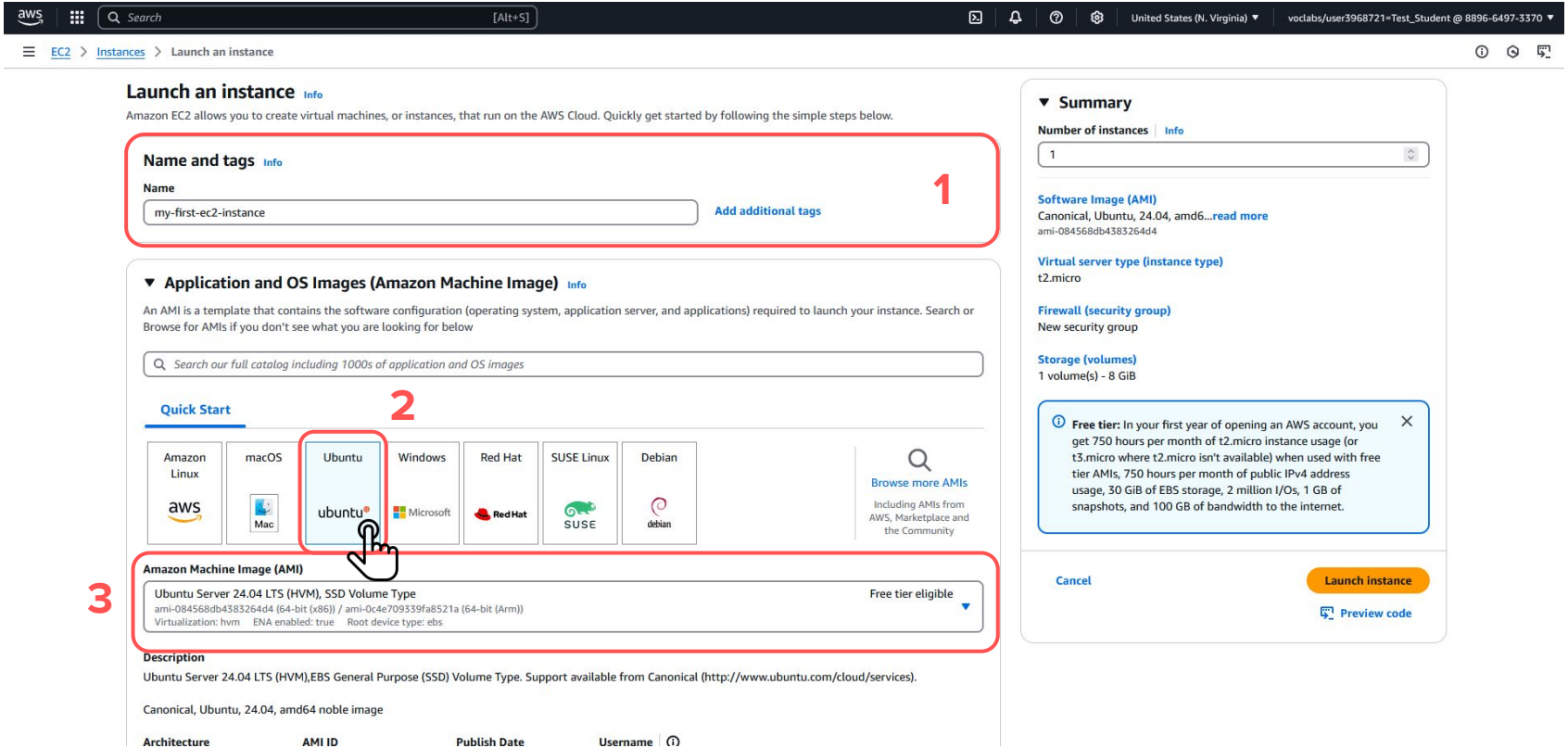
Searching for the EC2 service



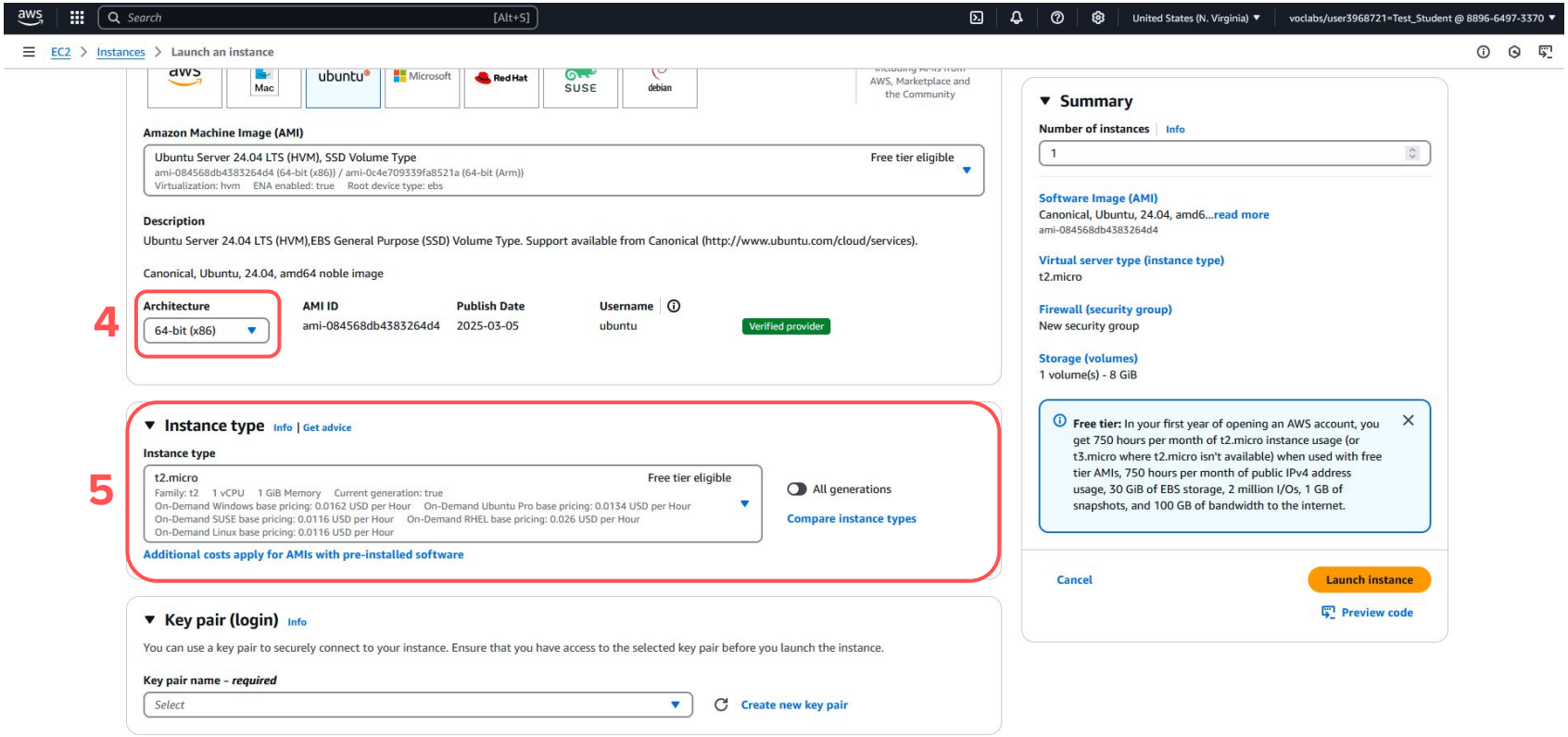
EC2 > Dashboard > Launch Instance



Give a name to you instance & select an OS image



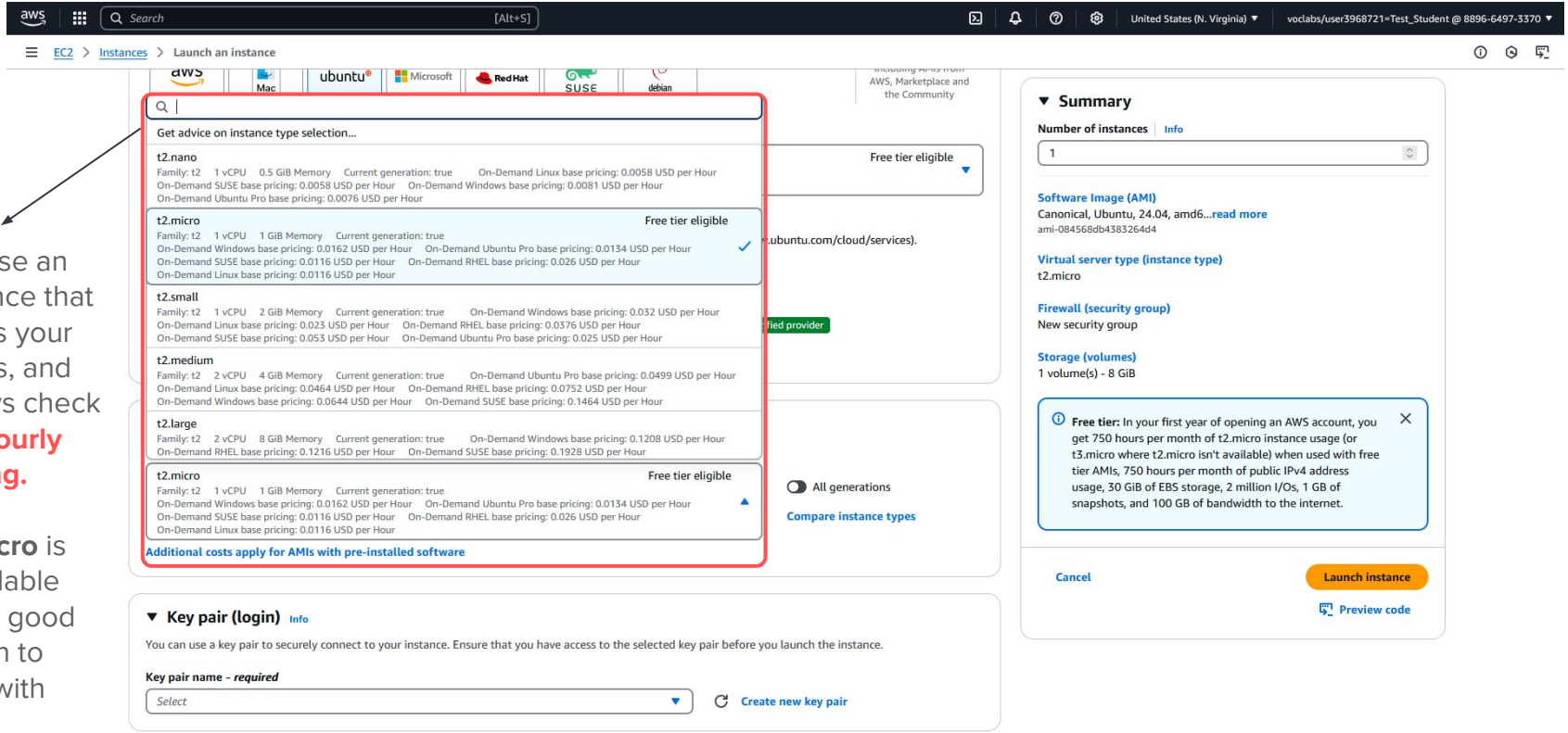
select Architecture & instance type



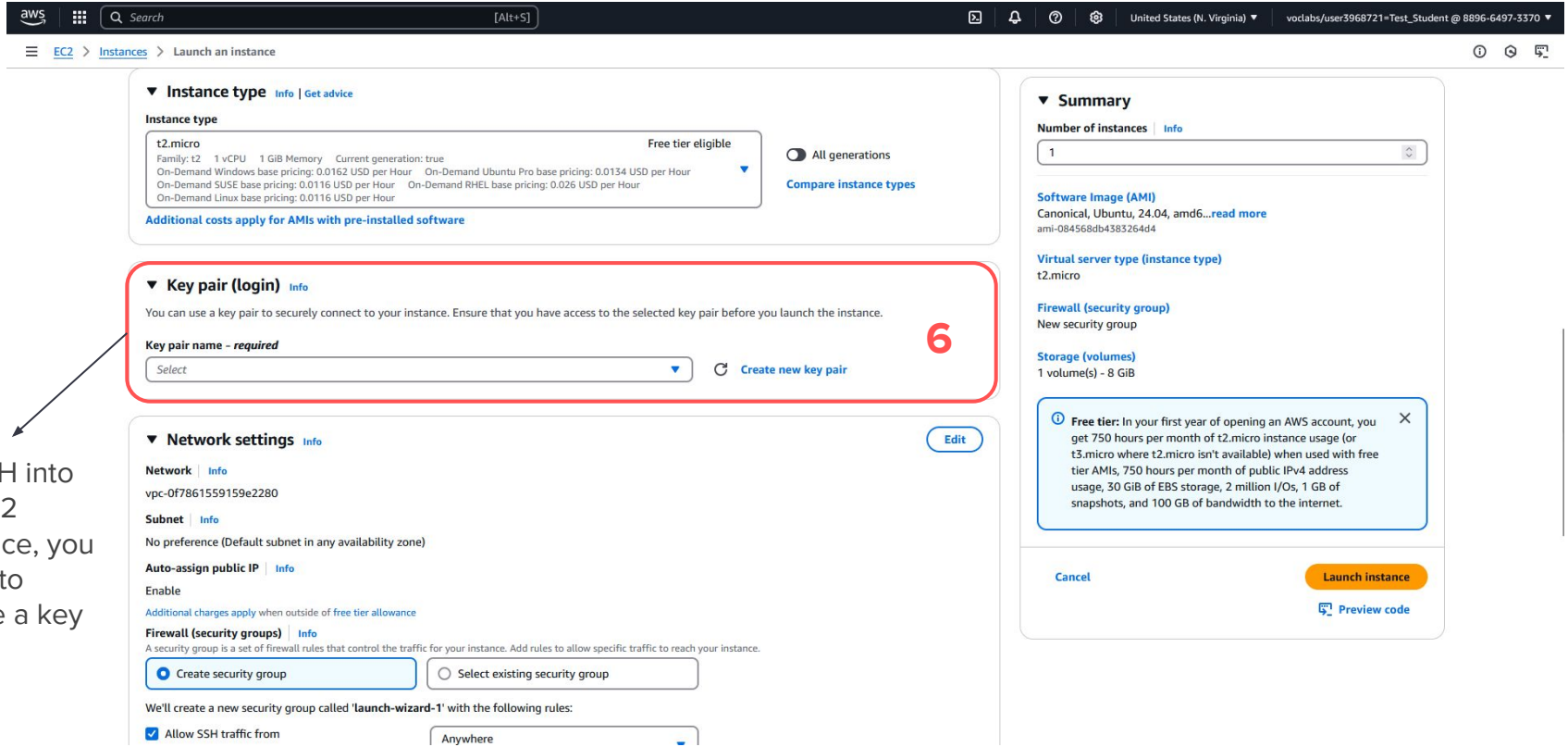
Different needs, different instance types

Choose an instance that meets your needs, and always check the **hourly pricing.**

t2.micro is affordable and a good option to start with

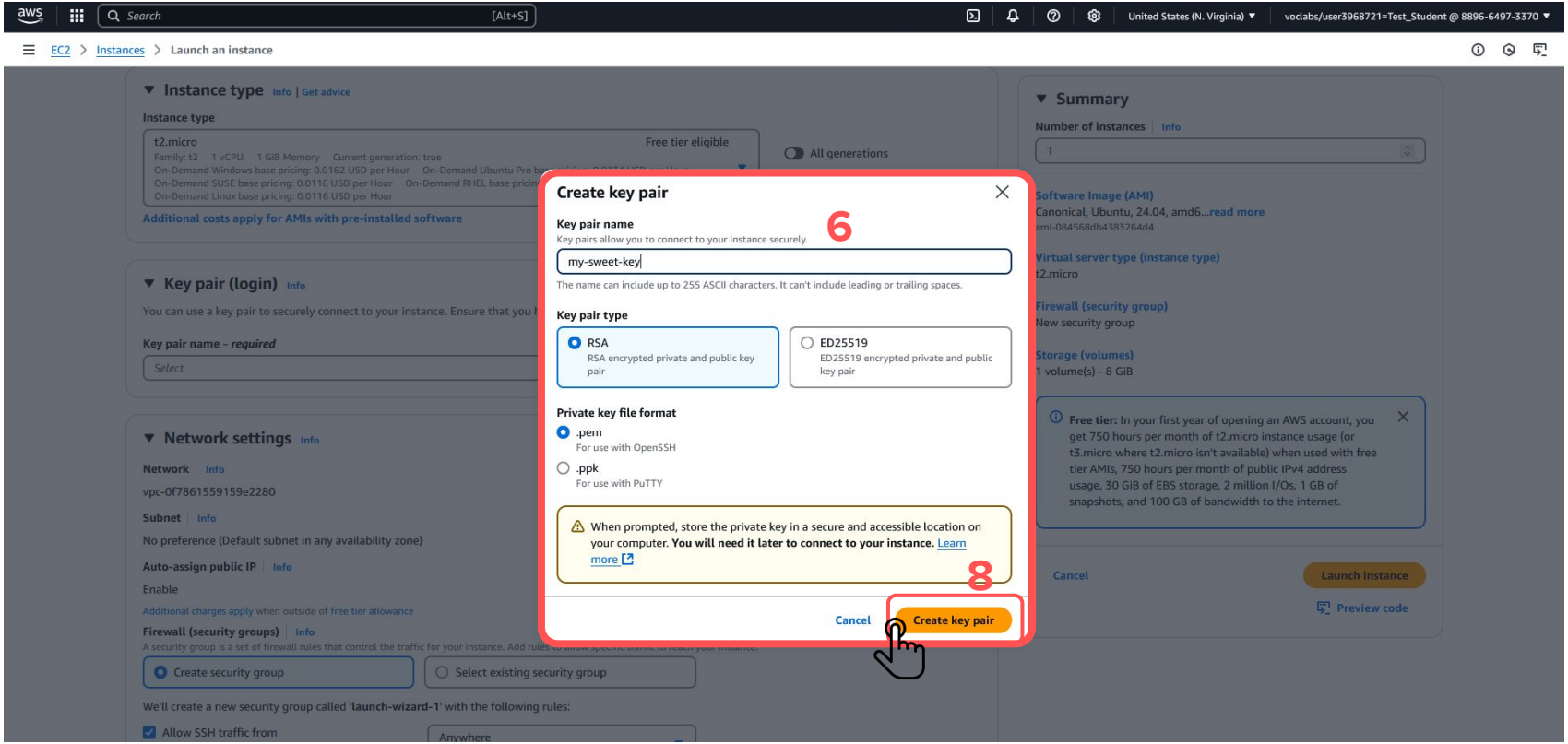


Prevent others to enter your EC2 instance



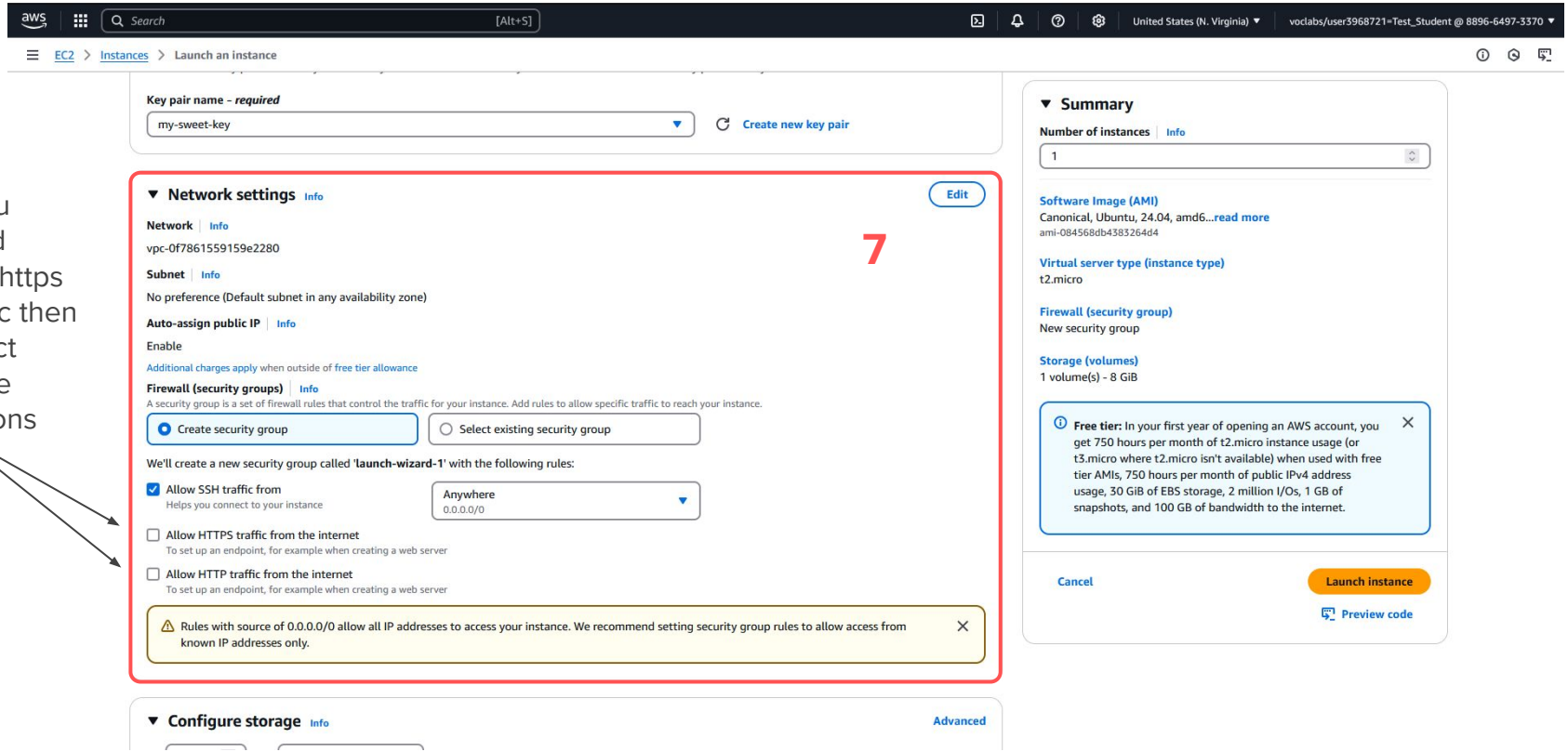
To SSH into an EC2 instance, you need to create a key pair

By creating a key



Network Settings

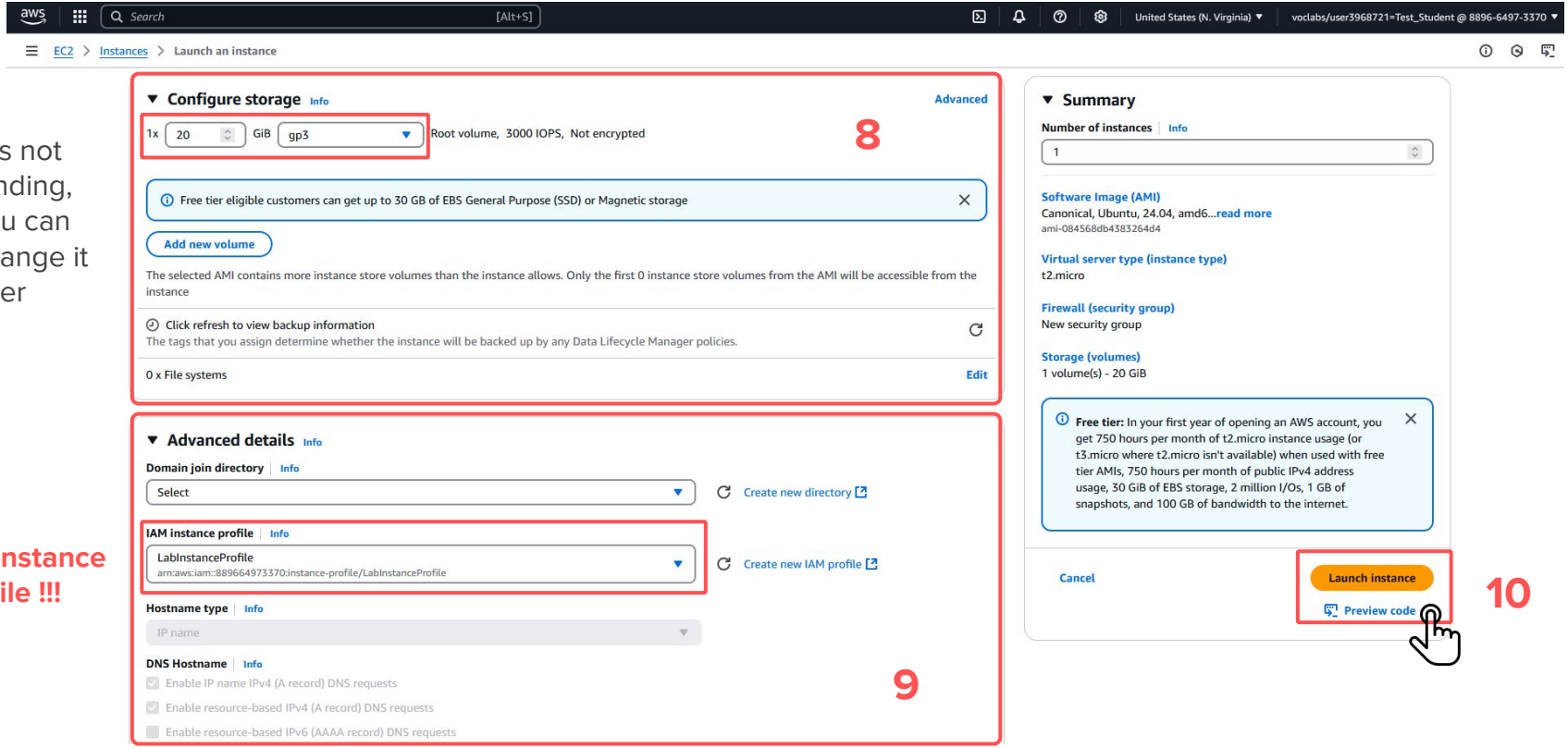
If you need http/https traffic then select these buttons



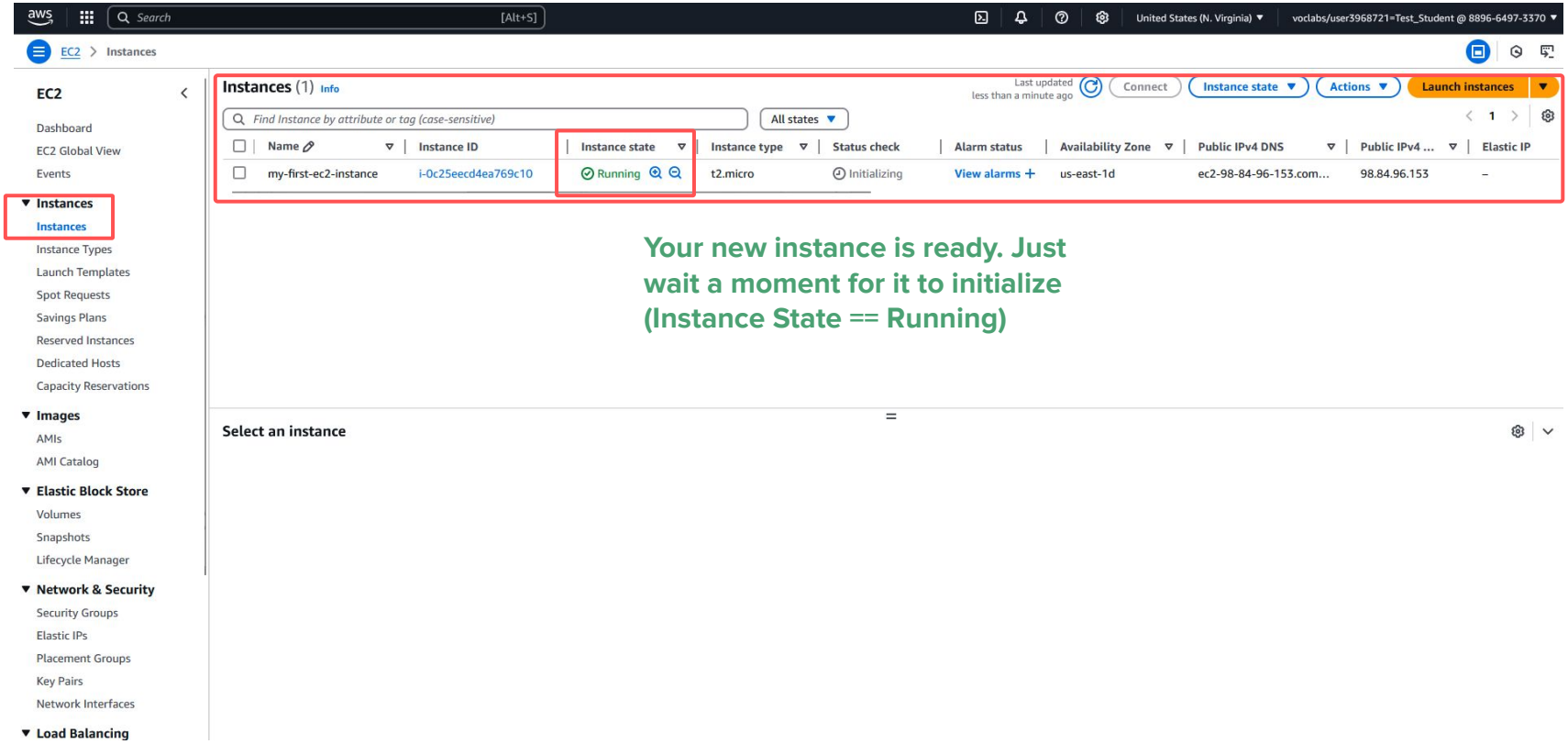
Configure storage

it is not binding, you can change it later

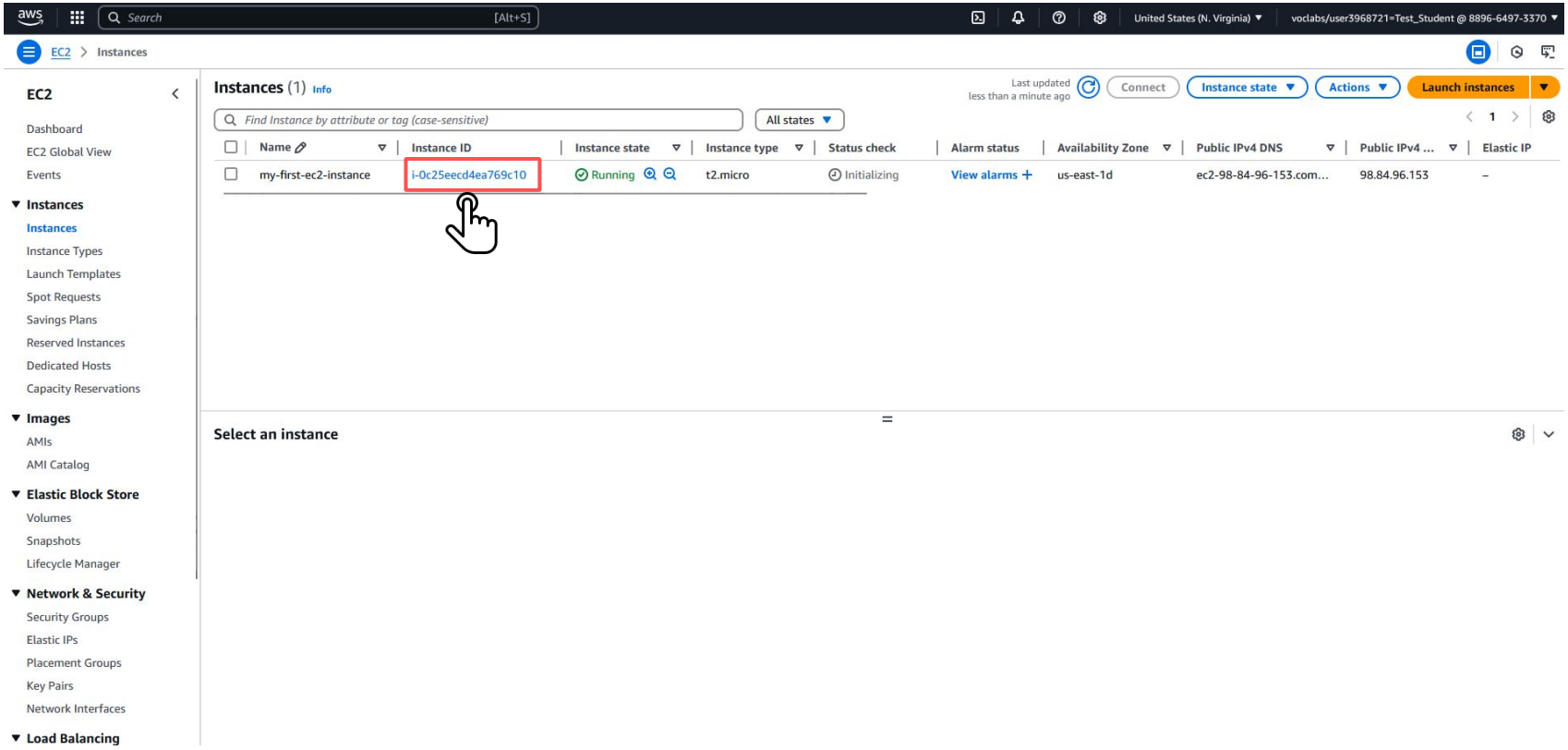
LabInstance Profile !!!



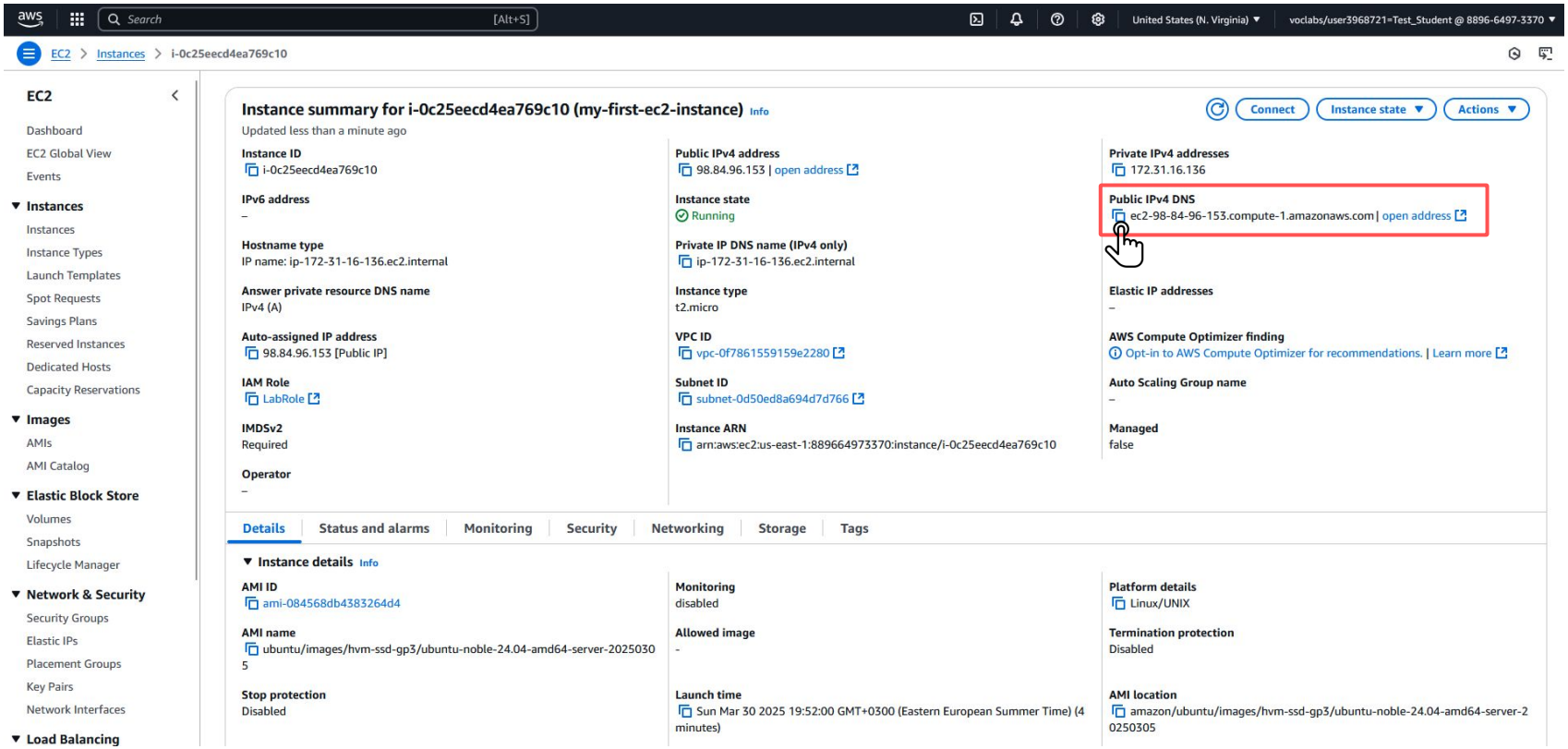
You just created the EC2 instance



Click on the Instance ID



This is the Dashboard of this specific EC2 instance



First attempt: ssh into the EC2 instance

```
[~/aws-keys]$ ssh -i my-sweet-key.pem ubuntu@ec2-98-84-96-153.compute-1.amazonaws.com
The authenticity of host 'ec2-98-84-96-153.compute-1.amazonaws.com (98.84.96.153)' can't be established.
ED25519 key fingerprint is SHA256:eC3WDea/qmgu4ieCikopzm9NsTP30QRGqL2j0OEtHSI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-98-84-96-153.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'my-sweet-key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "my-sweet-key.pem": bad permissions
ubuntu@ec2-98-84-96-153.compute-1.amazonaws.com: Permission denied (publickey).
[~/aws-keys]$
```

To avoid this issue you need to set the correct permissions for the .pem key

> chmod 600 my-sweet-key.pem
> ssh -i my-sweet-key.pem ubuntu@ec2-98-84-96-153.compute-1.amazonaws.com

Warning: the procedure on Windows is a bit different (check here:)

Second attempt: You did it :)

```
[~/aws-keys]$ ssh -i my-sweet-key.pem ubuntu@ec2-98-84-96-153.compute-1.amazonaws.com
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1024-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Mar 30 17:03:54 UTC 2025

  System load:  0.0               Processes:             104
  Usage of /:   9.2% of 18.33GB   Users logged in:       0
  Memory usage: 21%               IPv4 address for enX0: 172.31.16.136
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-16-136:~$ ls
ubuntu@ip-172-31-16-136:~$
```

Don’t forget to update/upgrade the instance

sudo apt update && sudo apt upgrade

Did we finish?

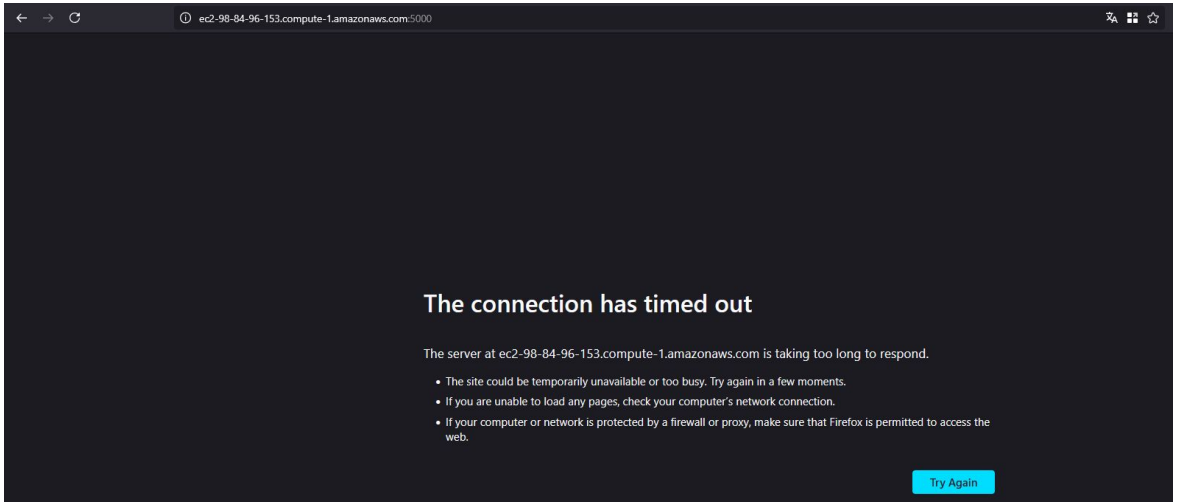
You may have an issue with ports later on

In this demo we will setup a flask server.

```
> sudo apt install python3-pip
> sudo apt install python3.12-venv
> python3 -m venv myenv
> source myenv/bin/activate
> pip install flask
> nano demo.py

> paste this code:
from flask import Flask

app = Flask(__name__)

@app.route('/')
def hello_world():
    return 'Hello, World!'

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```

Let’s start a flask server listening on port 5000

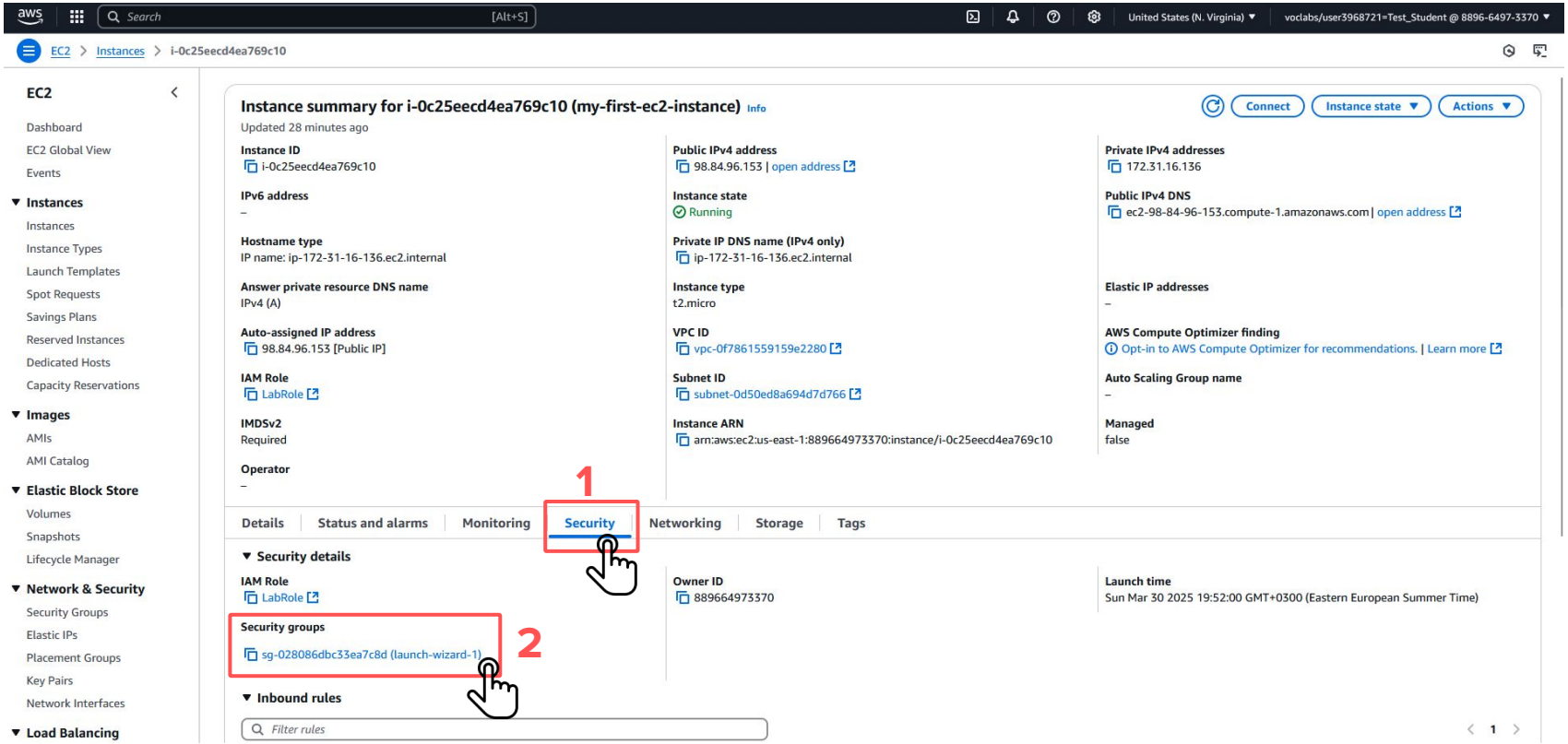
```
(myenv) ubuntu@ip-172-31-16-136:~$ python3 demo.py
 * Serving Flask app 'demo'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://172.31.16.136:5000
Press CTRL+C to quit
```



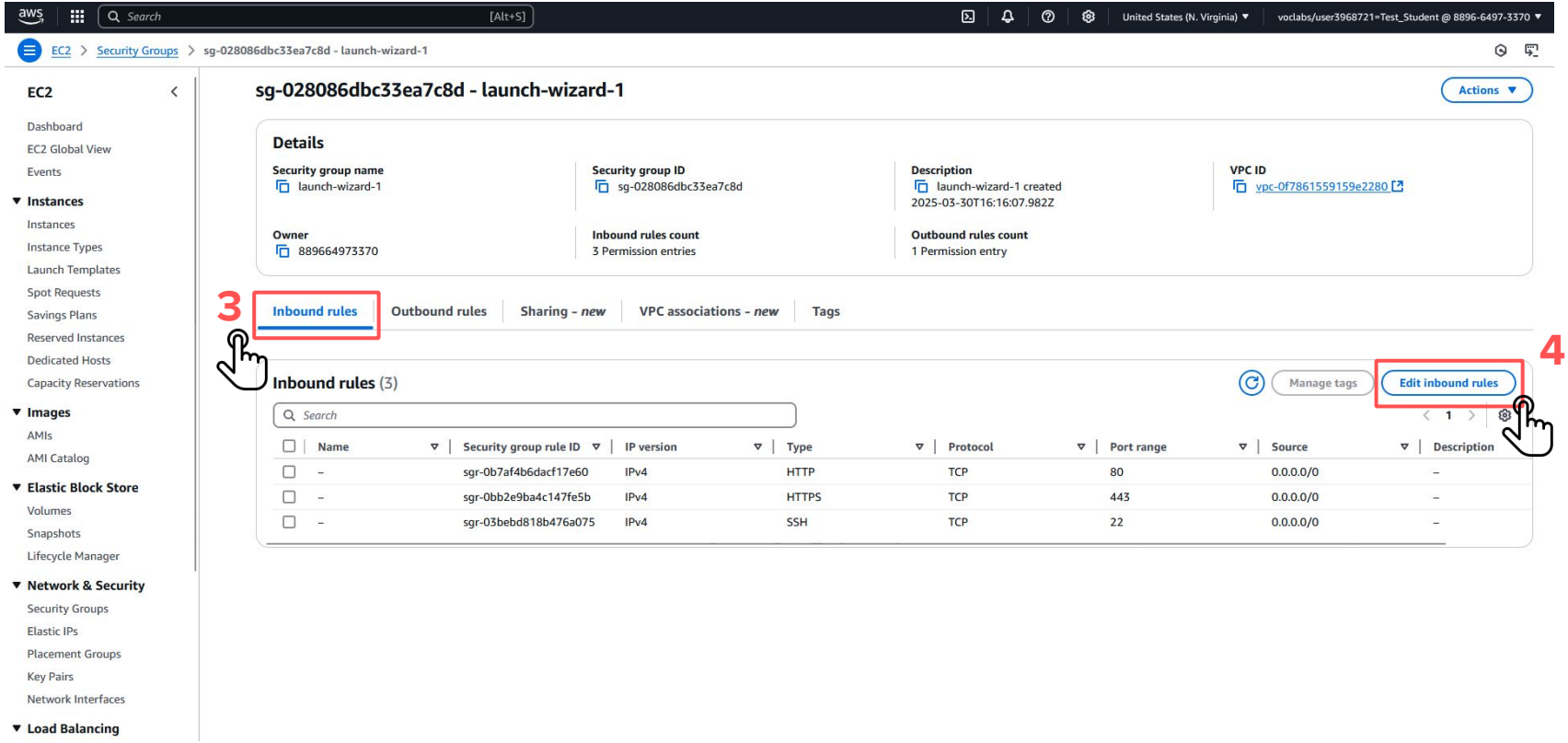
We didn't receive any response because of AWS's **Least Privilege Principle**. By default, all inbound traffic is blocked.

Next slide fixes this issue

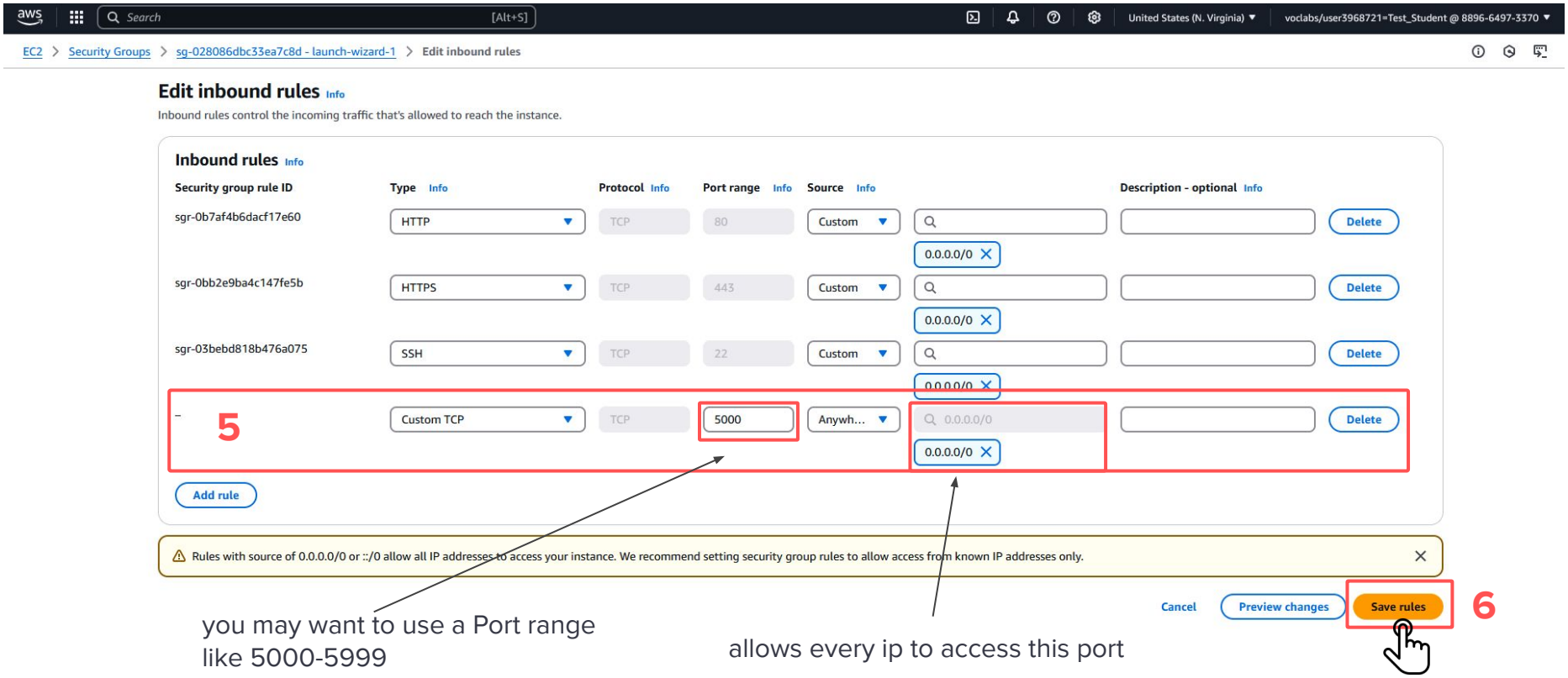
Activate the required port (5000 in our example)

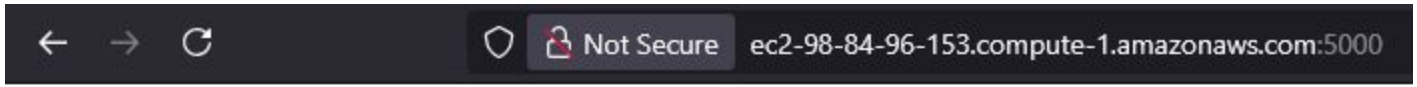


Edit inbound rules



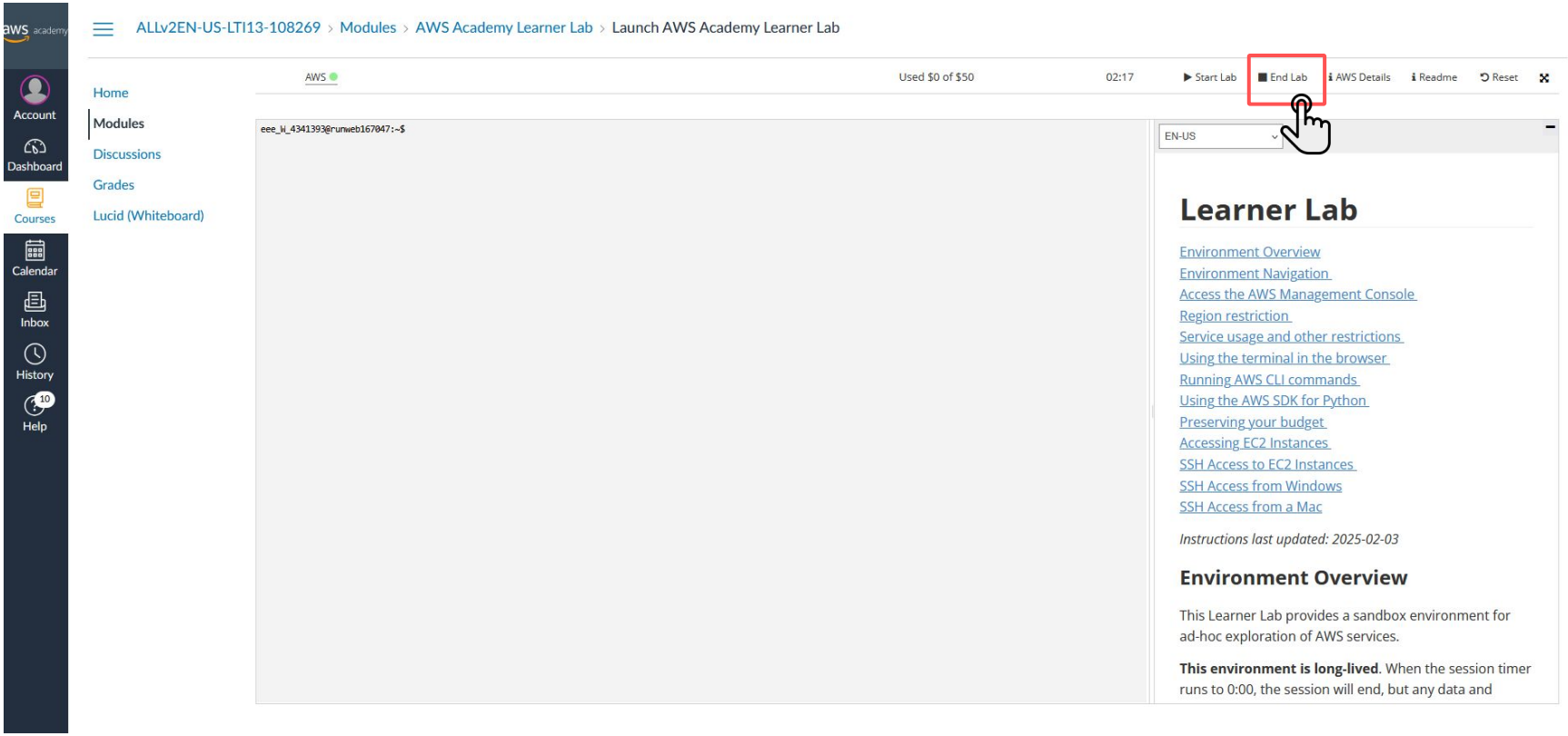
Add a rule


Edit inbound rules Info
Inbound rules control the incoming traffic that's allowed to reach the instance.
Inbound rules Info
Security group rule ID
Type Info
Protocol Info
Port range Info
Source Info
Description - optional Info
sgr-0b7af4b6dacf17e60
HTTP
TCP
80
Custom
0.0.0.0/0
Delete
sgr-0bb2e9ba4c147fe5b
HTTPS
TCP
443
Custom
0.0.0.0/0
Delete
sgr-03bebd818b476a075
SSH
TCP
22
Custom
0.0.0.0/0
Delete
5
Custom TCP
TCP
5000
Anywh...
0.0.0.0/0
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.
Cancel
Preview changes
Save rules
6
you may want to use a Port range like 5000-5999
allows every ip to access this port



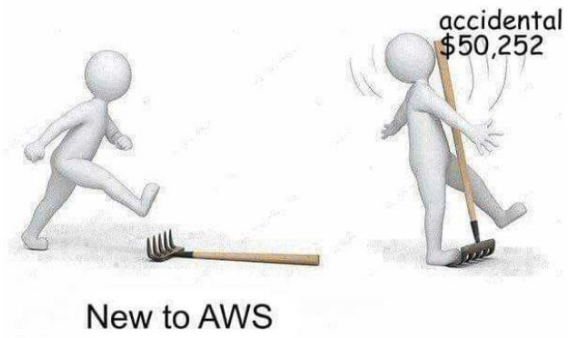
Hello, World!

Don’t forget to end lab session



Used $50 of $50

Thank you,
for your attention !!!



Tips

- re-clicking "Start Lab" resets the timer to 4 hours. It may be useful to do this before the current session ends
- When you finish, be sure to end the lab, time is money
- If you can’t reach your web service, check the security group settings
- You may not have access to certain EC2 instances due to academic account restrictions.