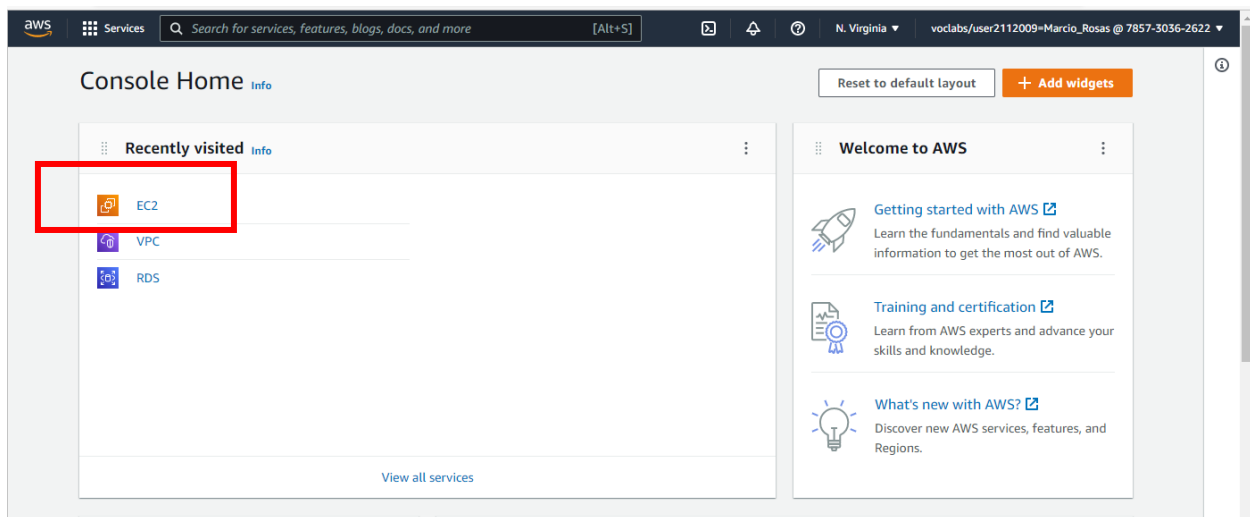


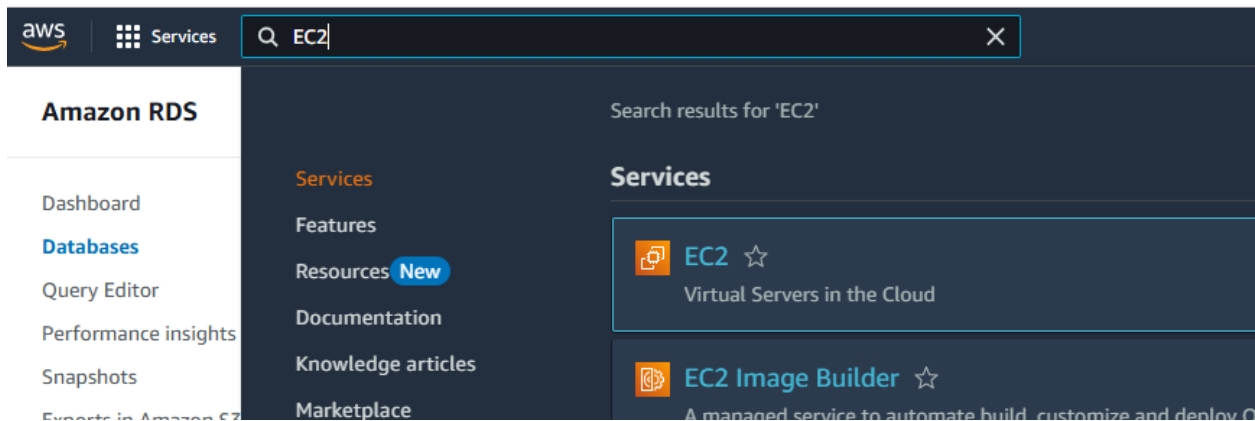
Creating EC2 Instance on AWS: Instructions

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

The screenshot displays the AWS Management Console for the EC2 service. The left-hand navigation pane lists various categories: Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area is titled 'You can change your default landing page for EC2.' and features a 'Permanently dismiss' button and a 'Change landing page' link. The 'Resources' section shows a summary of EC2 resources in the 'United States (N. Virginia)' region, including Instances (running), Dedicated Hosts, Key pairs, Security groups, Auto Scaling Groups, Elastic IPs, Load balancers, Snapshots, Capacity Reservations, Instances, Placement groups, and Volumes. The 'Launch instance' section provides instructions on how to get started and includes a 'Launch instance' button (highlighted with a red box) and a 'Migrate a server' link. The 'Service health' section shows the status of the EC2 service as 'operating normally'. The 'Zones' section lists available zones and their IDs. The 'Instance alarms' section shows that there are no alarms. The 'Scheduled events' section shows that there are no scheduled events. The 'Migrate a server' section provides information on using the AWS Application Migration Service. The 'Quick ID filter' section is also visible. On the right side, the 'Account attributes' section shows the default VPC and settings. The 'Explore AWS' section provides links to various AWS resources and documentation. The 'Additional information' section provides links to the AWS website, documentation, and support.

Resources

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

Resource	Count
Instances (running)	0
Dedicated Hosts	0
Key pairs	1
Security groups	2
Auto Scaling Groups	0
Elastic IPs	0
Load balancers	0
Snapshots	0
Capacity Reservations	0
Instances	0
Placement groups	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 United States (N. Virginia) Region

Instance alarms

[View in CloudWatch](#)

0 in alarm 0 OK 0 insufficient data

Scheduled events

United States (N. Virginia)

No scheduled events

Migrate a server

Use AWS Application Migration Service to simplify and expedite migration from physical, virtual, and cloud infrastructure to AWS.

[Get started with AWS Application Migration Service](#)

Service health

Region: United States (N. Virginia)

Status: [AWS Health Dashboard](#)

This service is operating normally.

Zones

Zone name	Zone ID
us-east-1a	use1-az5
us-east-1b	use1-az1
us-east-1c	use1-az2
us-east-1d	use1-az4
us-east-1e	use1-az3
us-east-1f	use1-az5

[Enable additional Zones](#)

Account attributes

Default VPC: vpc-Gu92180304e2d33c2

Settings: Data protection and security, Allowed AMIs, Zones, EC2 Serial Console, Default credit specification, EC2 console preferences

Explore AWS

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. [Learn more](#)

Get Up to 40% Better Price Performance

Tag instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. [Learn more](#)

Optimize EC2 Cost with Spot Instances and EC2 Auto Scaling

Get started with EC2 Spot Instances, EC2 Auto Scaling, and Launch Templates by following this step-by-step tutorial. [Learn more](#)

Additional information

[Get started walkthroughs](#)

[Getting started guide](#)

[Documentation](#)

[All EC2 resources](#)

[Forums](#)

[Pricing](#)

[Contact us](#)

In the next screen, choose:

Application and OS Images (Amazon Machine Image)

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-052064a798f08f0d63 (64-bit (x86), uefi-preferred) / ami-089f6a798d0c2548a (64-bit (x86), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.9.20250929.0 x86_64 HVM kernel-6.1

Architecture 64-bit (x86) **Boot mode** uefi-preferred **AMI ID** ami-052064a798f08f0d63 **Publish Date** 2025-09-25 **Username** ec2-user **Verified provider**

Instance type

t3.micro
Family t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour On-Demand SUSE base pricing: 0.0104 USD per Hour
On-Demand Linux base pricing: 0.0104 USD per Hour On-Demand RHEL base pricing: 0.0192 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour

Additional costs apply for AMIs with pre-installed software

Summary

Number of instances 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d63

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Launch Instance

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

Key pair (login)

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

Select **Create new key pair**

Network settings

Network vpc-0a92380304e2d33c2

Subnet No preference (Default subnet in any availability zone)

Auto-assign public IP Enable

Firewall (security groups)

Create security group Select existing security group

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

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

keypair_miniproject_2025

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type



☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel

Create key pair

This will download a .pem file to your computer. Move this pem 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:

aws

Search

[Option+5]

United States (N. Virginia)

Account ID: 7675-6610-6422

notahy/ami-0321a60c - Instance_Type - Sebastian, V...

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

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-052064a7b8009f0d

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

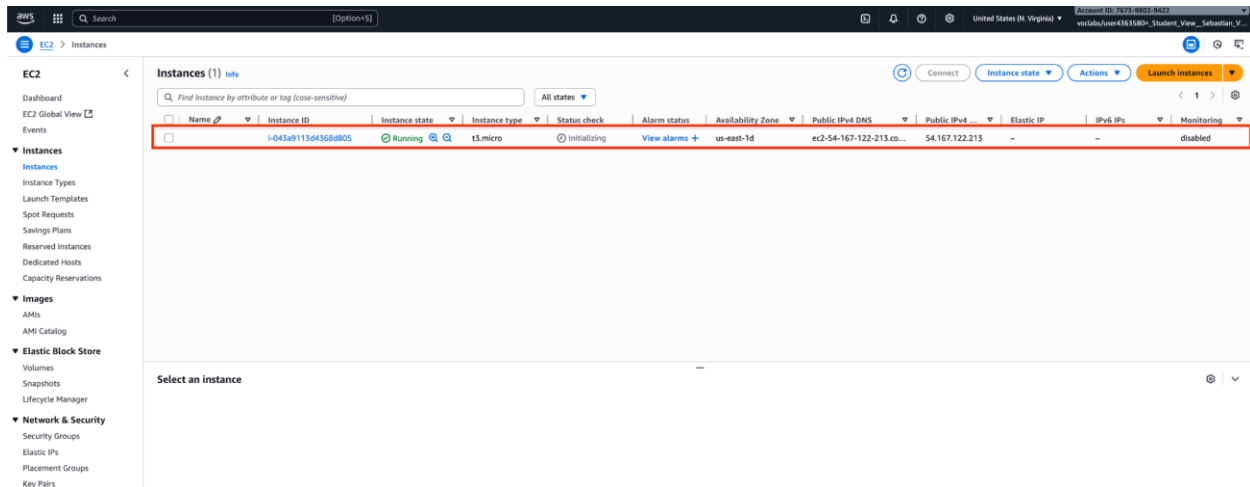
After that, click “launch instance” using the orange button on the right section of the screen:

The screenshot shows the AWS Management Console 'Launch an instance' page. The 'Network settings' section is expanded, showing 'vpc-0a92380304e2d33c2' as the VPC and 'No preference' as the subnet. The 'Firewall (security groups)' section has 'Create security group' selected. The 'Configure storage' section shows '1x 8 GiB gp3' as the root volume. The 'Launch Instance' button is highlighted with an orange box in the 'Summary' section.

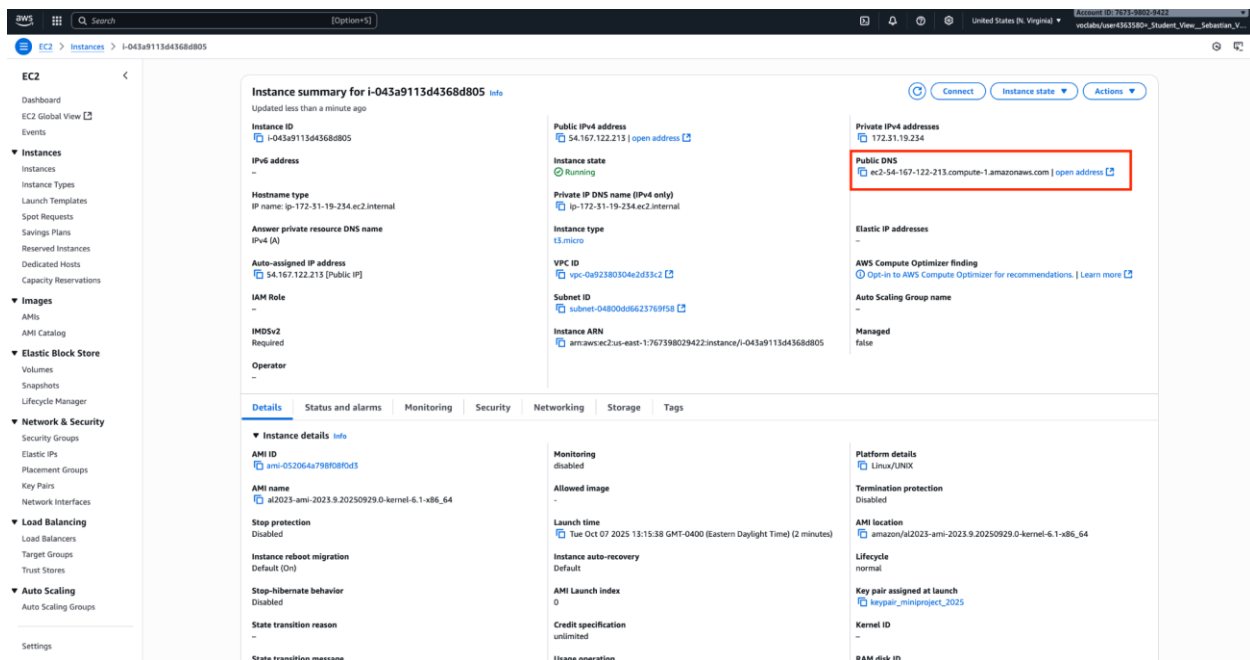
You will see this screen below, confirming your EC2 instance has been correctly launched. Click on the highlighted area to navigate to your EC2 dashboard.

The screenshot shows the AWS Management Console 'Launch an instance' page after a successful launch. A green banner at the top displays the message: "Success Successfully initiated launch of instance i-043a9113d4d68d805". Below the banner, there are several "Next Steps" cards for configuring the instance, such as "Create billing usage alerts", "Connect to your instance", "Connect an RDS database", "Create EBS snapshot policy", "Manage detailed monitoring", "Create Load Balancer", "Create AWS budget", "Manage CloudWatch alarms", "Disaster recovery for your instances", "Monitor for suspicious runtime activities", "Get instance screenshot", and "Get system log". The "View all instances" button is highlighted with an orange box at the bottom right.

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:

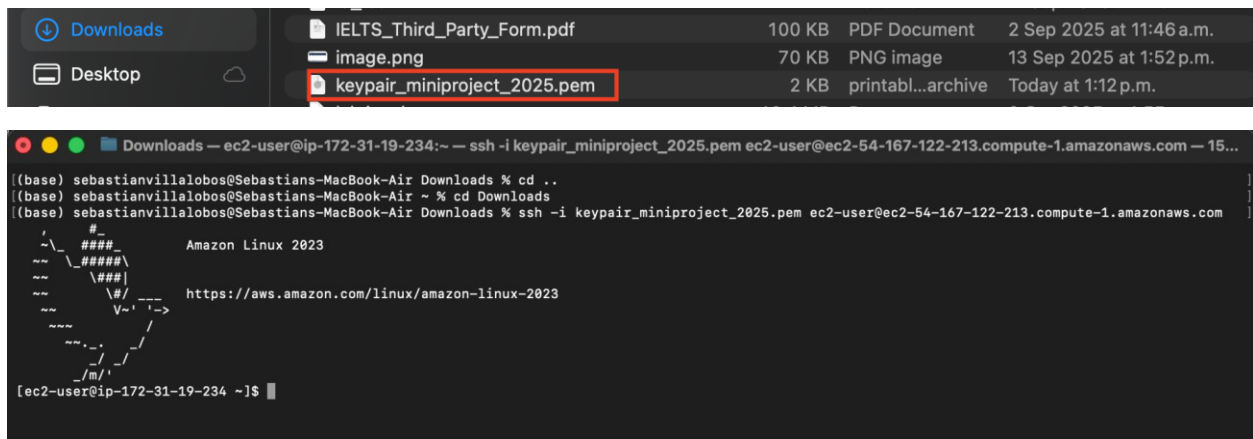
- keep in mind that, regarding `ssh/your_keypair_name.pem` and `your_public_IPv4`:

- **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

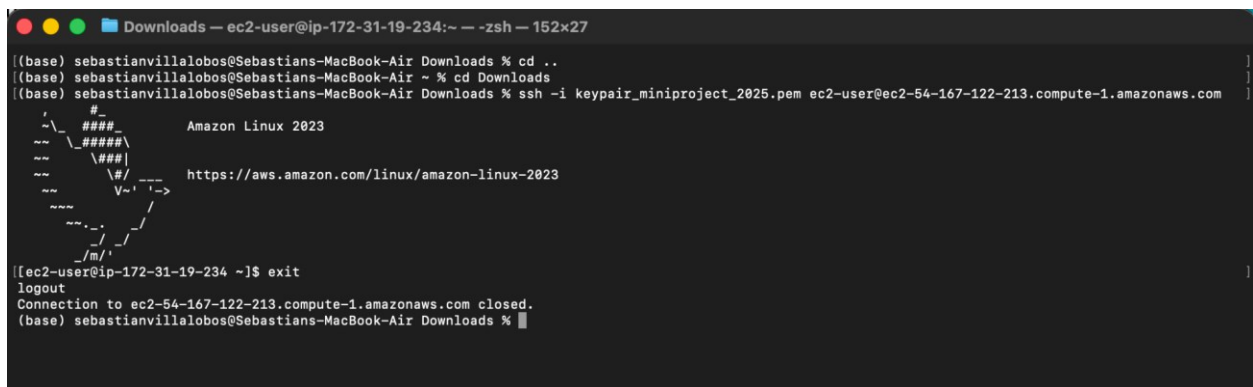
Command: `ssh -i "path_to_your_file"/your_keypair_name.pem ec2-user@your_public_IPv4`

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:


```
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
```

```
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
dlopen ssh/keypair_miniproject_2024.pem failed: The specified module could not be found.
The authenticity of host 'ec2-3-208-15-237.compute-1.amazonaws.com (3.208.15.237)' can't be established.
ED25519 key fingerprint is SHA256:wN/koUVkczqlZe0OqhF5sSwrvGVF4eRQhqbIwGRgZ3k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

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

```
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.
~~~   \#/
~~~    V~'  ->
~~~~~  /
~~~~~ _/_/_/
~~~~~ _/m/'

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 ~]$
```

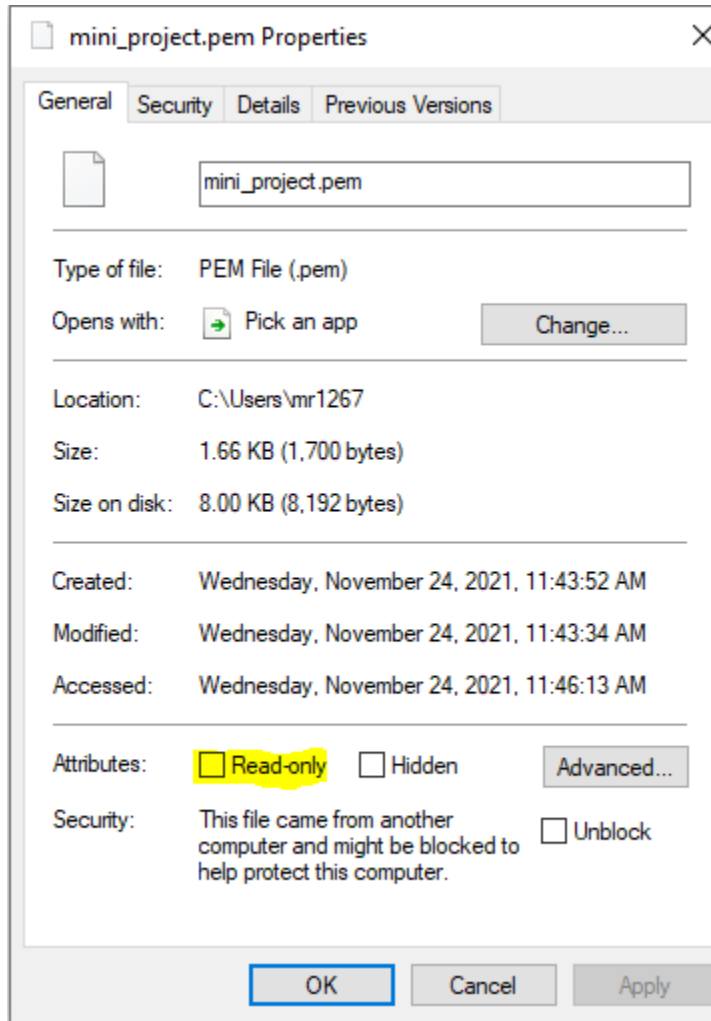
Once you see this screen, logout from the EC2 by typing “exit” with go back from the Ec2 to your computer (terminal or Power Shell) and then return to the to the Mini-project Instructions.

[illegible]

Troubleshooting:

Windows users:

You may need to change the permissions of your `_keypair.pem` file to read 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` file must 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.