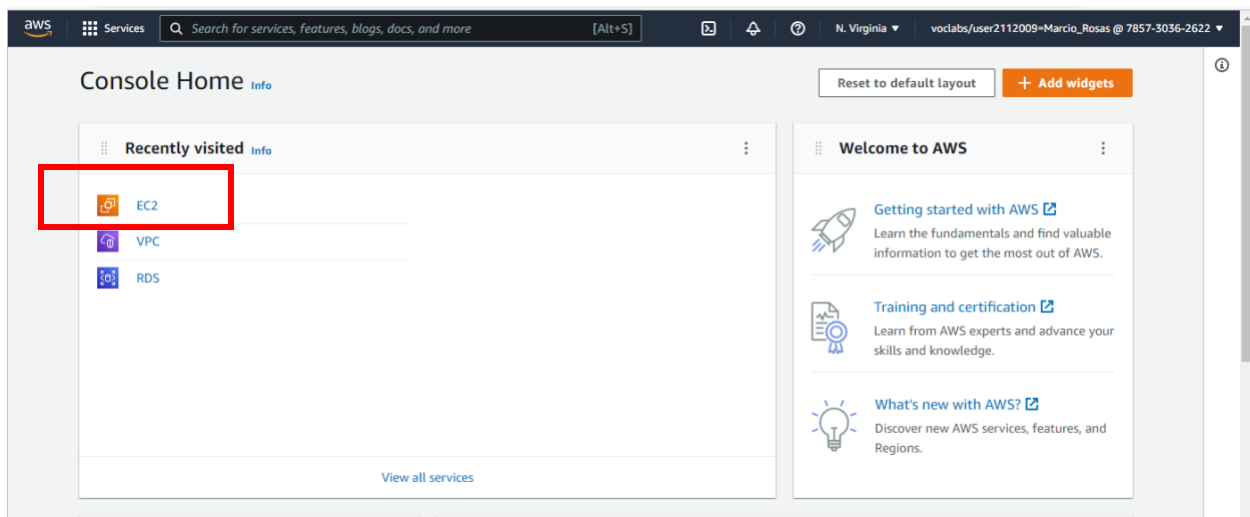


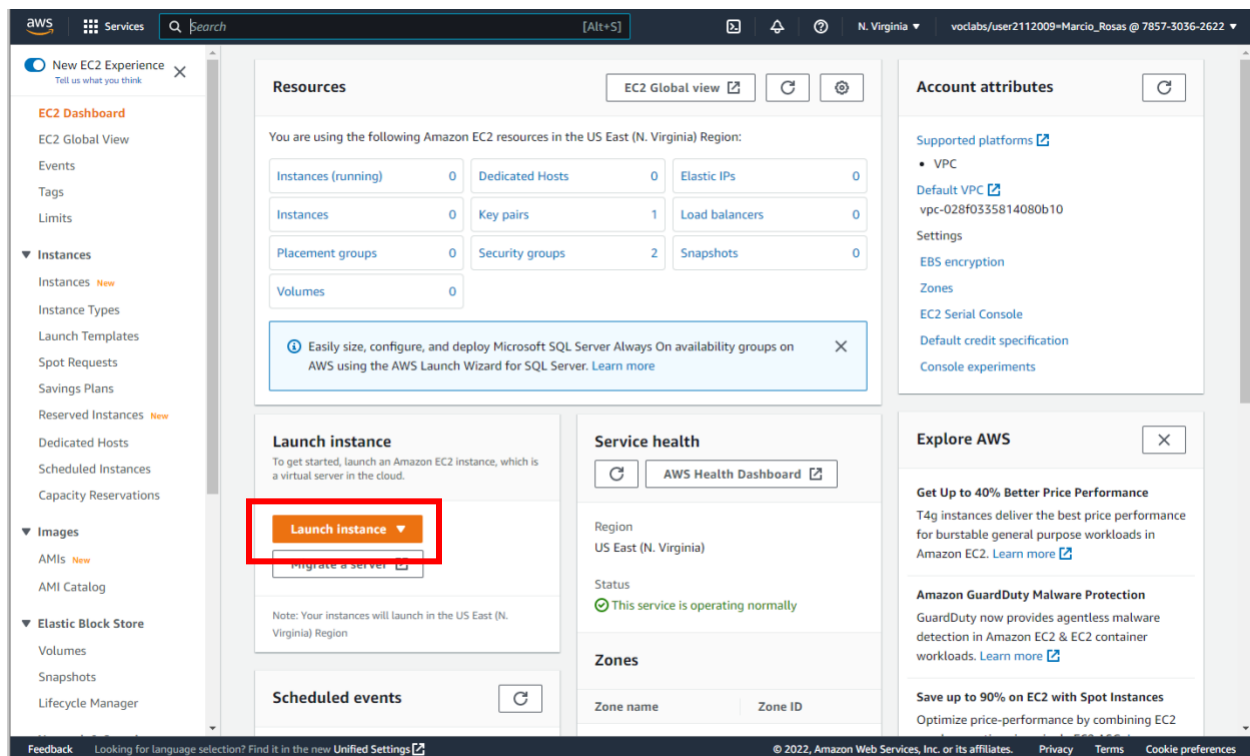
Creating EC2 Instance on AWS: Instructions

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:



From the console dashboard, choose Launch Instance



In the next screen, choose:

Amazon Linux 2 AMI (HVM), Kernel 5.10, SSD Volume Type as the AMI, as shown below:

Services Search [Alt+S] N. Virginia voclabs/user2112009=Marcio_Rosas @ 7857-3036-2622

EC2 > Instances > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name [Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Quick Start

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

S

[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type Free tier eligible

ami-09d3b3274b6c5d4aa (64-bit (x86)) / ami-081dc0707789c2daf (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2

Architecture AMI ID

64-bit (x86) ami-09d3b3274b6c5d4aa Verified provider

▼ Summary

Number of instances [Info](#)

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...[read more](#)
ami-09d3b3274b6c5d4aa

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel [Launch Instance](#)

Scroll down and select t2.micro as instance type:

▼ Instance type [Info](#)

Instance type

t2.micro Free tier eligible

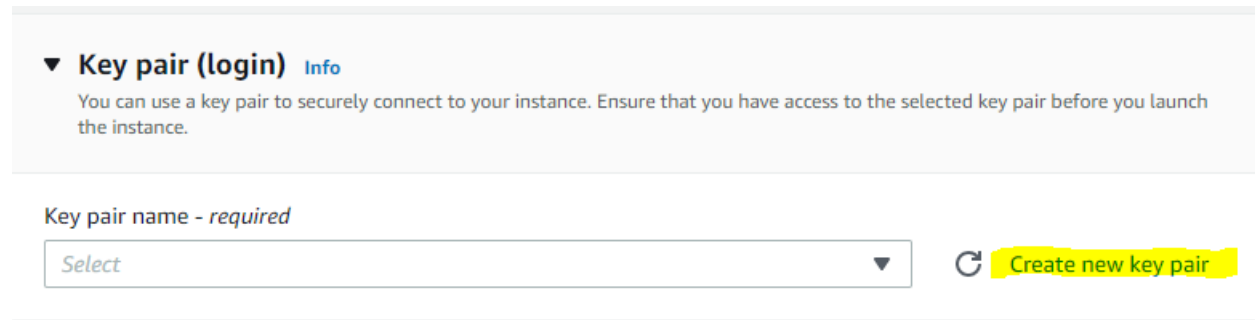
Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

[Compare instance types](#)

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



▼ **Key pair (login)** [Info](#)

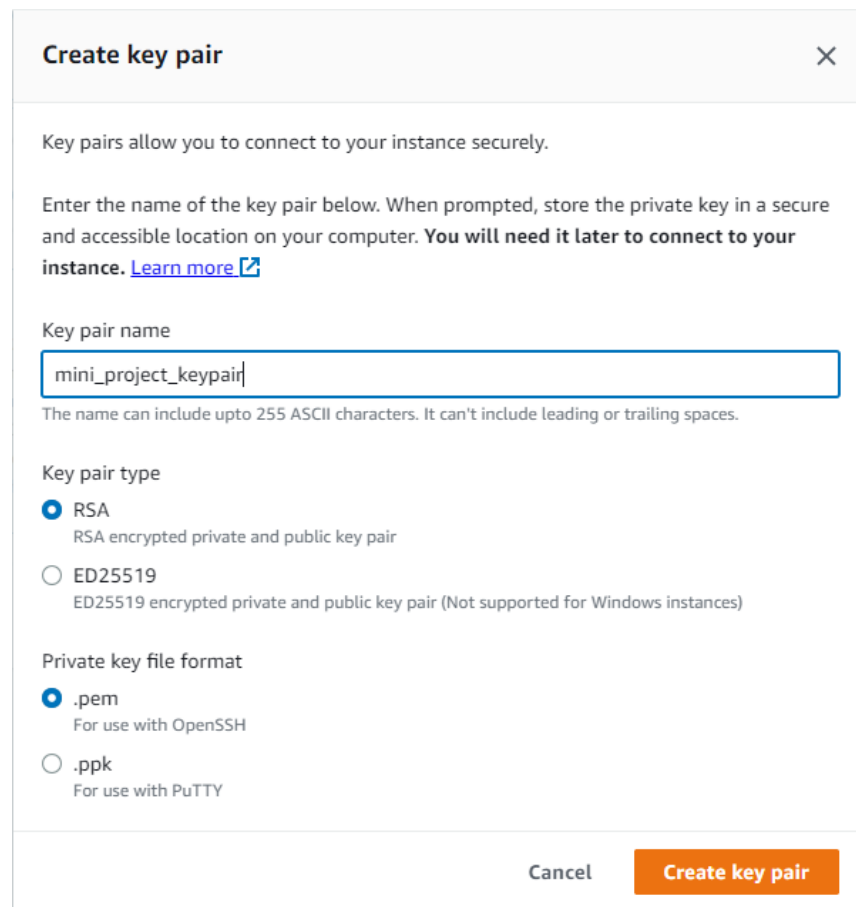
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

↻ **Create new key pair**

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 pairs allow you to connect to your instance securely.

Enter the name of the key pair below. 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](#) ↗

Key pair name

mini_project_keypair

The name can include upto 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 (Not supported for Windows instances)

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

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:

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-028f0335814080b10

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. 

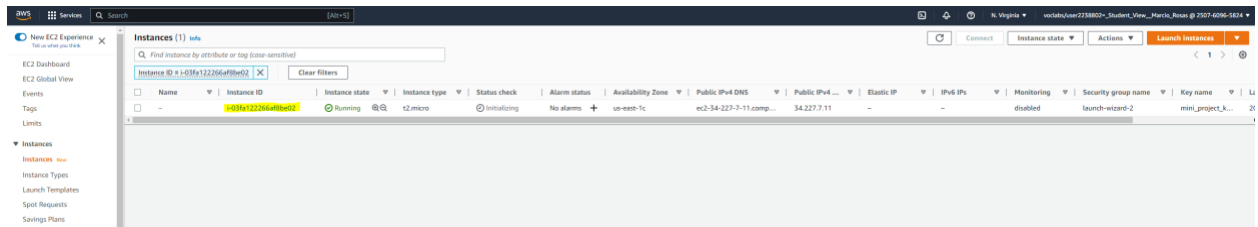
After that, click “launch instance” using the orange button on the right section of the screen:

The screenshot shows the 'Launch Instance' wizard in the AWS Management Console, specifically the 'Network settings' page. The page is divided into two main sections: 'Network settings' on the left and 'Summary' on the right. In the 'Network settings' section, the 'Network' is set to 'vpc-028f0335814080b10', the 'Subnet' is 'No preference (Default subnet in any availability zone)', and 'Auto-assign public IP' is 'Enable'. Under 'Firewall (security groups)', the 'Create security group' option is selected. A message states: 'We'll create a new security group called 'launch-wizard-1' with the following rules:'. Below this, there are three rules: 'Allow SSH traffic from' (checked, source 'Anywhere'), 'Allow HTTPS traffic from the internet' (unchecked), and 'Allow HTTP traffic from the internet' (unchecked). A warning message at the bottom of the rules section states: '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.' In the 'Summary' section, the 'Number of instances' is '1', the 'Software Image (AMI)' is 'Amazon Linux 2 Kernel 5.10 AMI...', the 'Virtual server type (instance type)' is 't2.micro', and the 'Firewall (security group)' is 'New security group'. The 'Storage (volumes)' section shows '1 volume(s) - 8 GiB'. At the bottom right, there are two buttons: 'Cancel' and 'Launch Instance'. The 'Launch Instance' button is highlighted with a red rectangle. A 'Free tier' notification box is also visible in the 'Summary' section, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.'

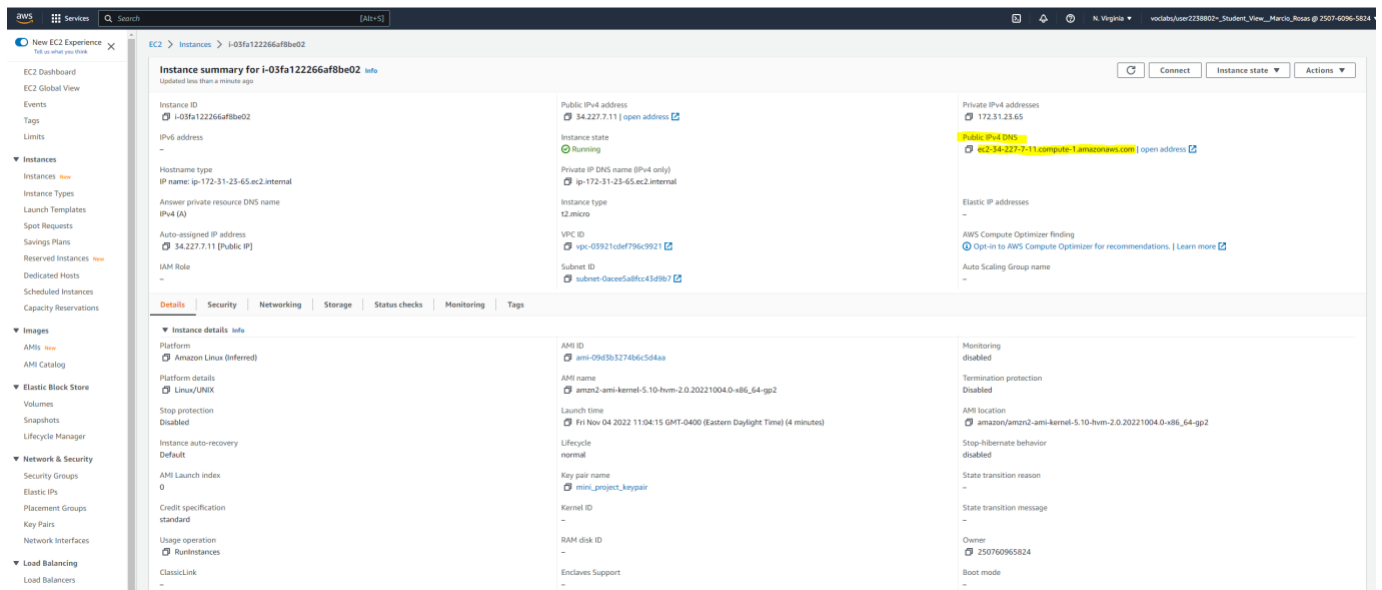
You will see this screen below, confirming your EC2 instance has been correctly launched. Click on the highlighted area to navigate to your EC2 dashboard.

The screenshot shows the 'Launch Instance' success page in the AWS Management Console. The page has a green header bar with a checkmark icon and the text 'Success Successfully initiated launch of instance i-05fa72226eaf8be02f'. Below this, there is a 'Launch log' link. The main content area is titled 'Next Steps' and contains three cards. The first card is 'Create billing and free tier usage alerts' with a 'Create billing alerts' button. The second card is 'Connect to your instance' with a 'Connect to instance' button and a 'Learn more' link. The third card is 'Connect an RDS database' with a 'Connect an RDS database' button and a 'Learn more' link. The 'Connect an RDS database' card also includes a 'Create a new RDS database' link.

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:

```
ssh -i ssh/your_keypair_name.pem ec2-user@your_public_IPv4
```

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.

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

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/mini_project_keypair.pem ec2-user@ec2-34-238-233-5.compute-1.amazonaws.com
```

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

```

 _ | _ | _ )
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-85-152 ~]$
```

Once you see this screen, logout from the EC2 by typing “exit” with go back to the Mini-project Instructions.

```
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/mini_project_keypair.pem ec2-user@ec2-34-238-233-5.compute-1.amazonaws.com
Last login: Fri Nov  4 15:47:40 2022 from pool-70-106-236-51.clppva.fios.verizon.net
Last login: Fri Nov  4 15:47:40 2022 from pool-70-106-236-51.clppva.fios.verizon.net

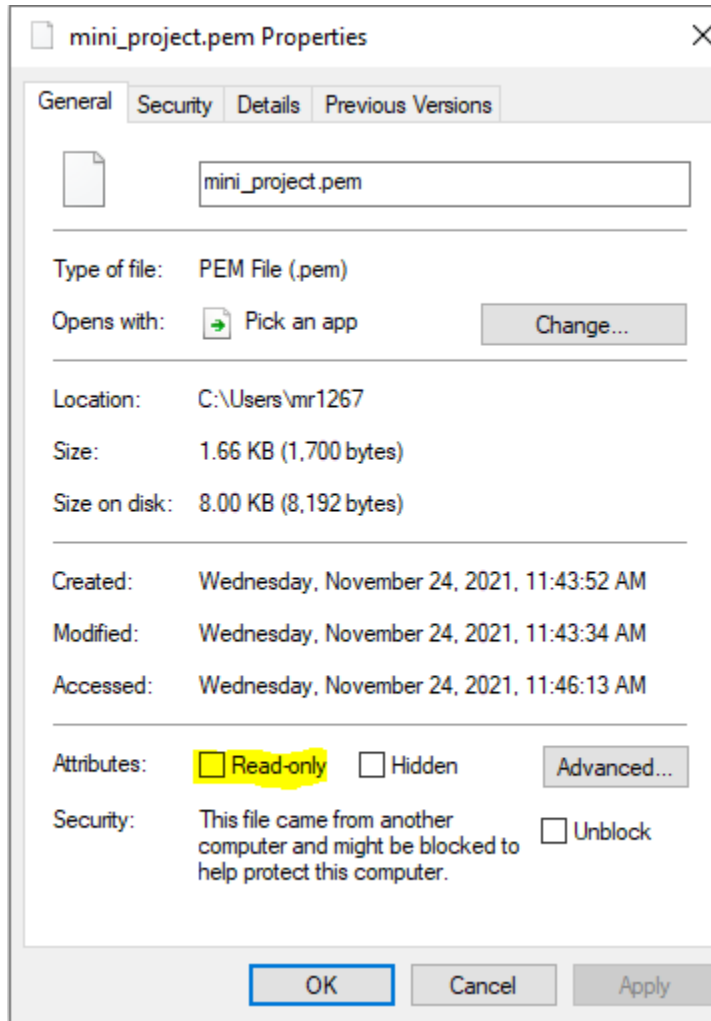
 _ | _ | _ )
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-85-152 ~]$ exit
logout
Connection to ec2-34-238-233-5.compute-1.amazonaws.com closed.
PS C:\Users\mr1267>
```

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.