Setting up an EC2 on AWS

If you do not have an AWS account, please go to…

https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/

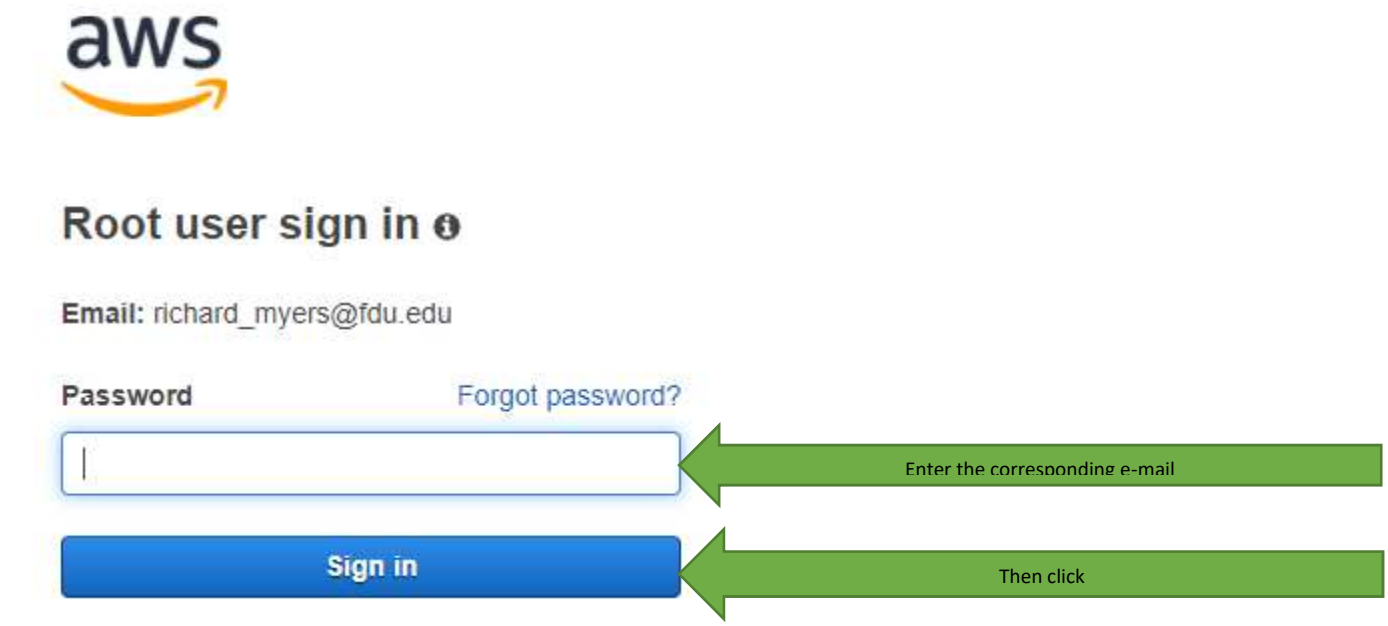
… and follow the instructions

EC2s are “Elastic Compute Cloud” provided by Amazon. They are not necessarily Linux based but in this class that’s what we will use. Please use these instructions to set yours up.

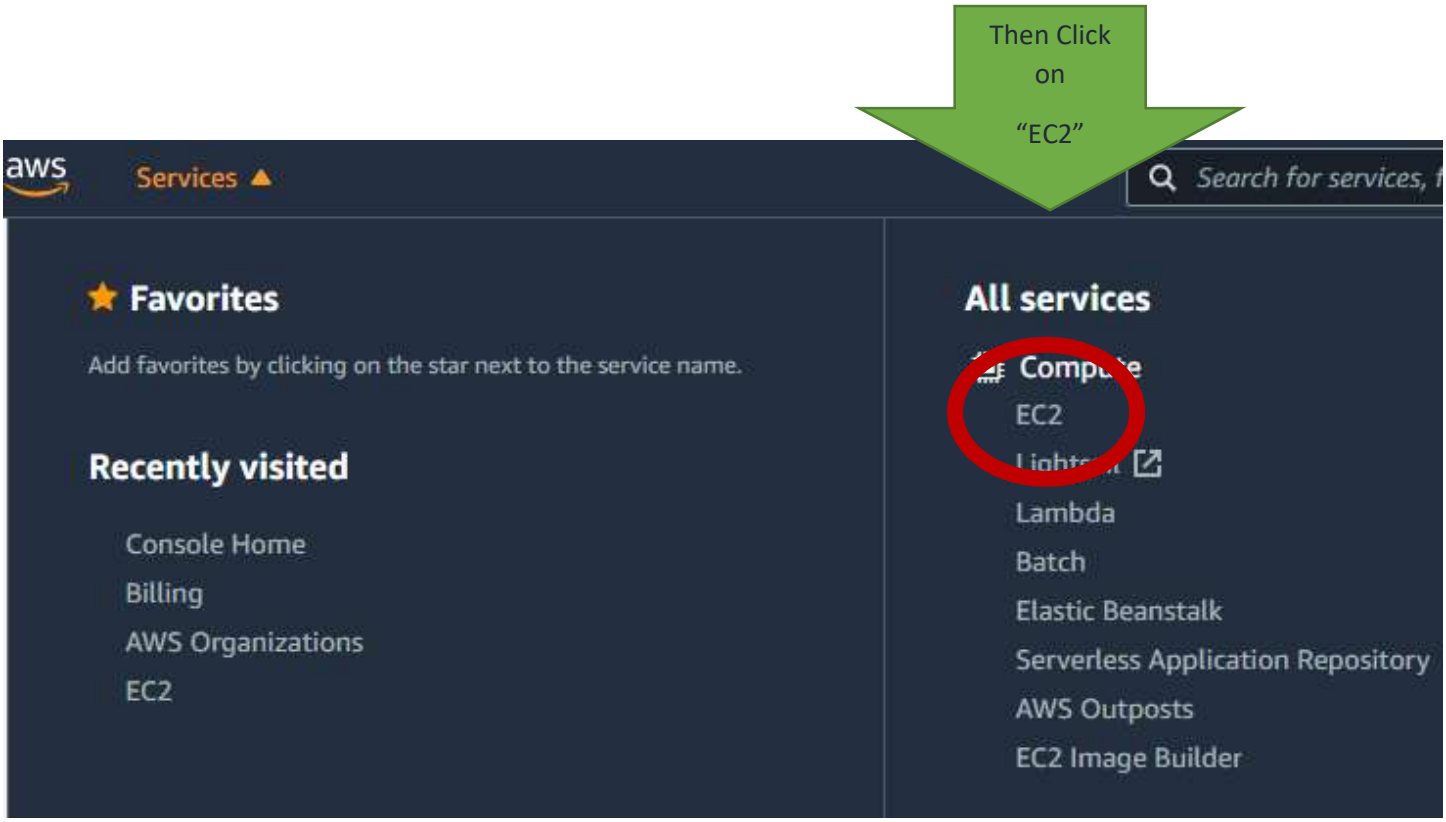
Go to website…

https://aws.amazon.com/console/

…and log in

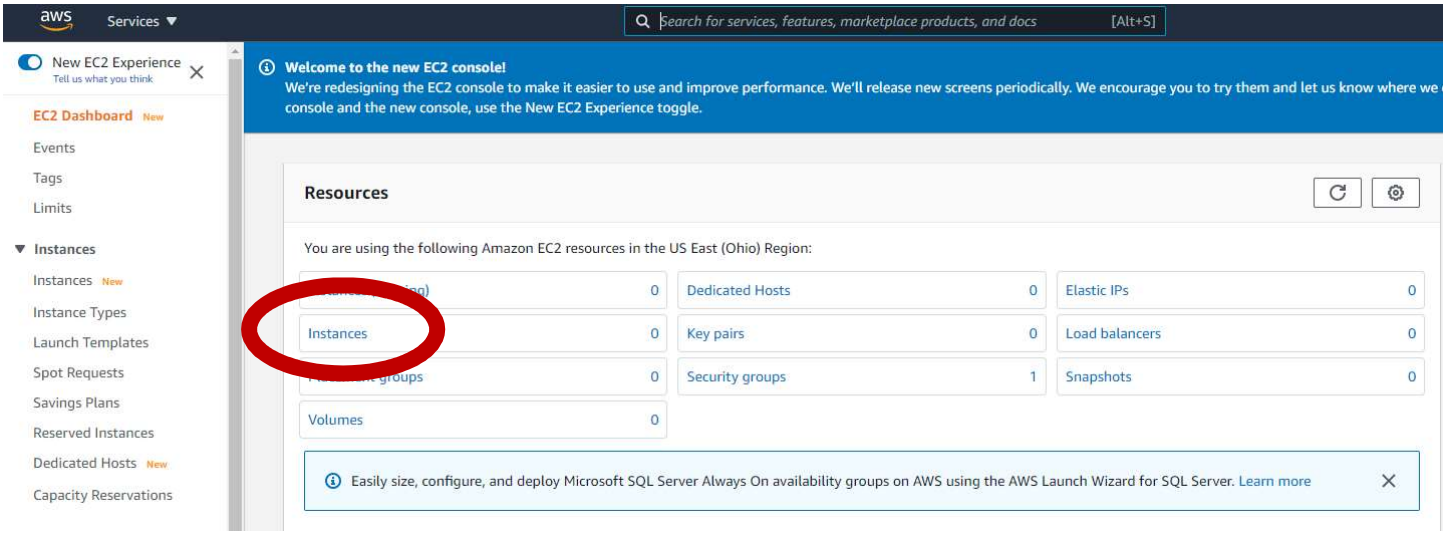

Root user sign in
Email: richard_myers@fdu.edu
Password
Forgot password?
Enter the corresponding e-mail
Sign in
Then click


Drop Down "Services"
aws
Services
profrich
Ohio
Support
AWS Management Console


Then Click on "EC2"
aws
Services
Search for services,
Favorites
Add favorites by clicking on the star next to the service name.
Recently visited
Console Home
Billing
AWS Organizations
EC2
All services
EC2
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository
AWS Outposts
EC2 Image Builder

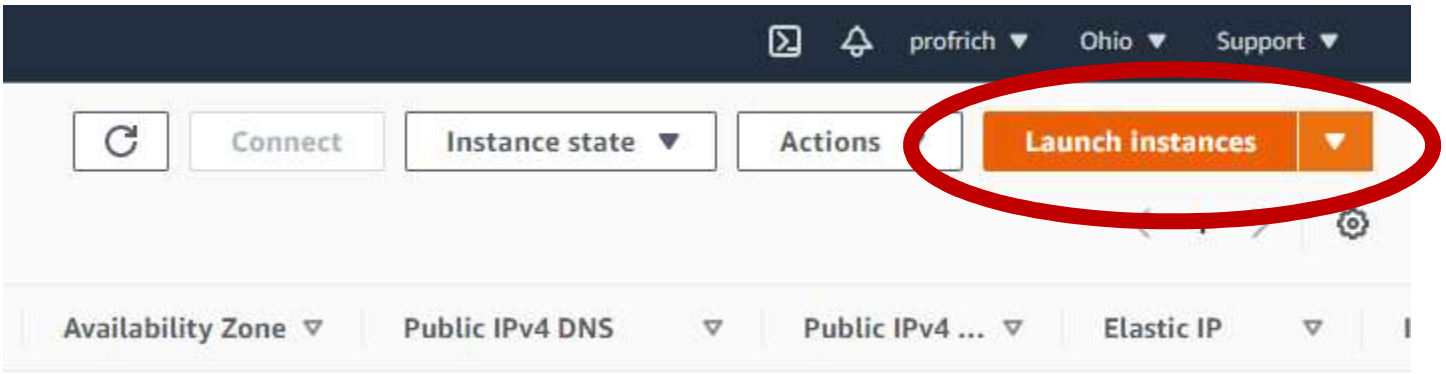
Then Click on

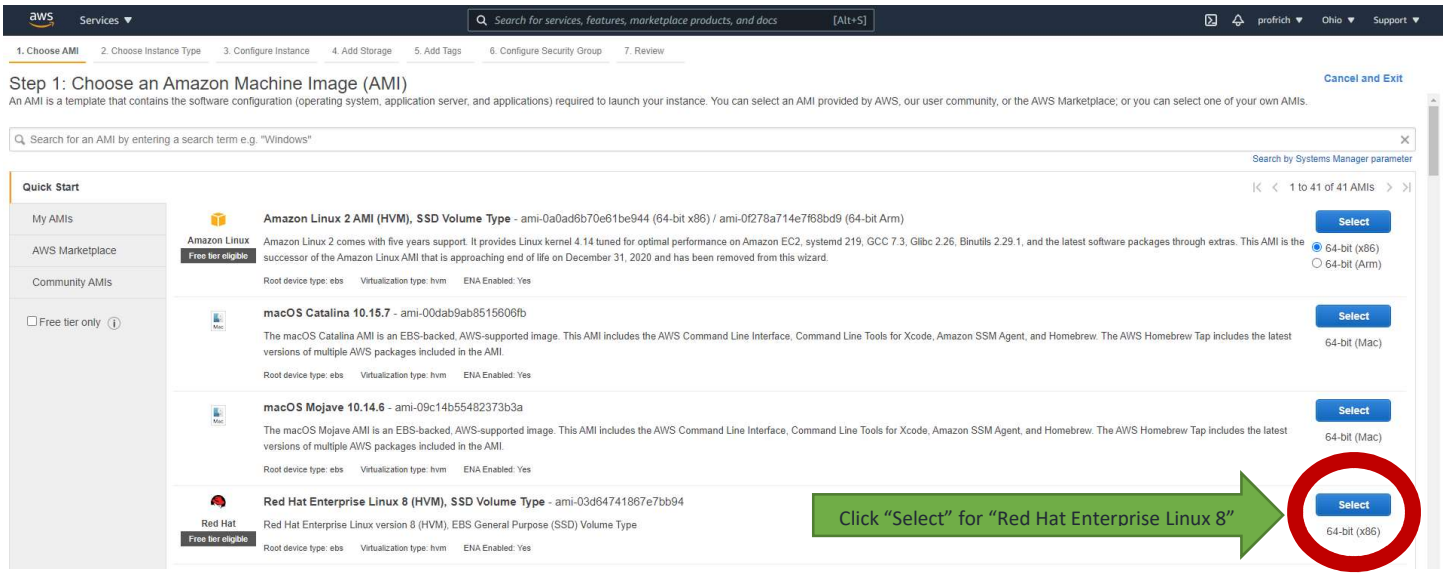
“Instances”

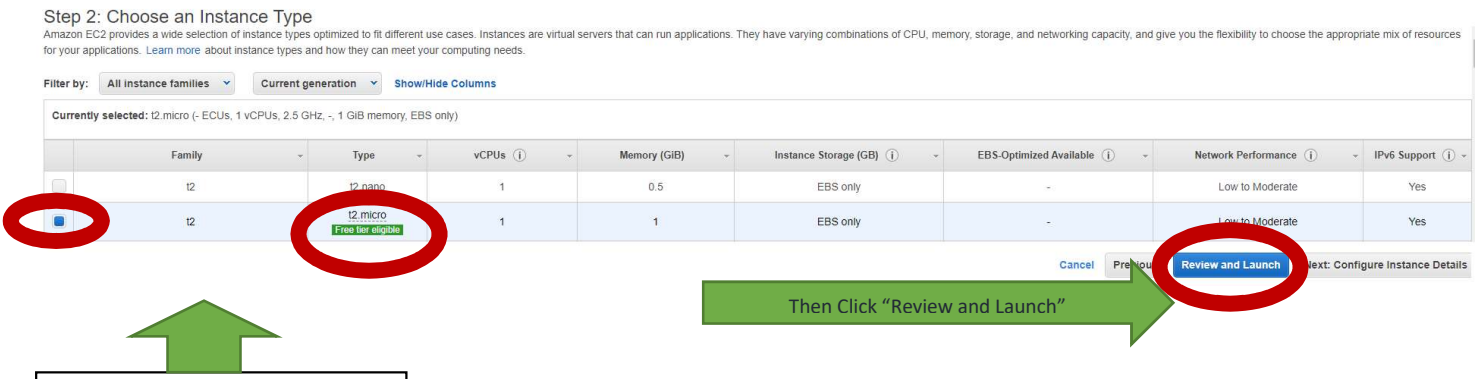


Then Click on

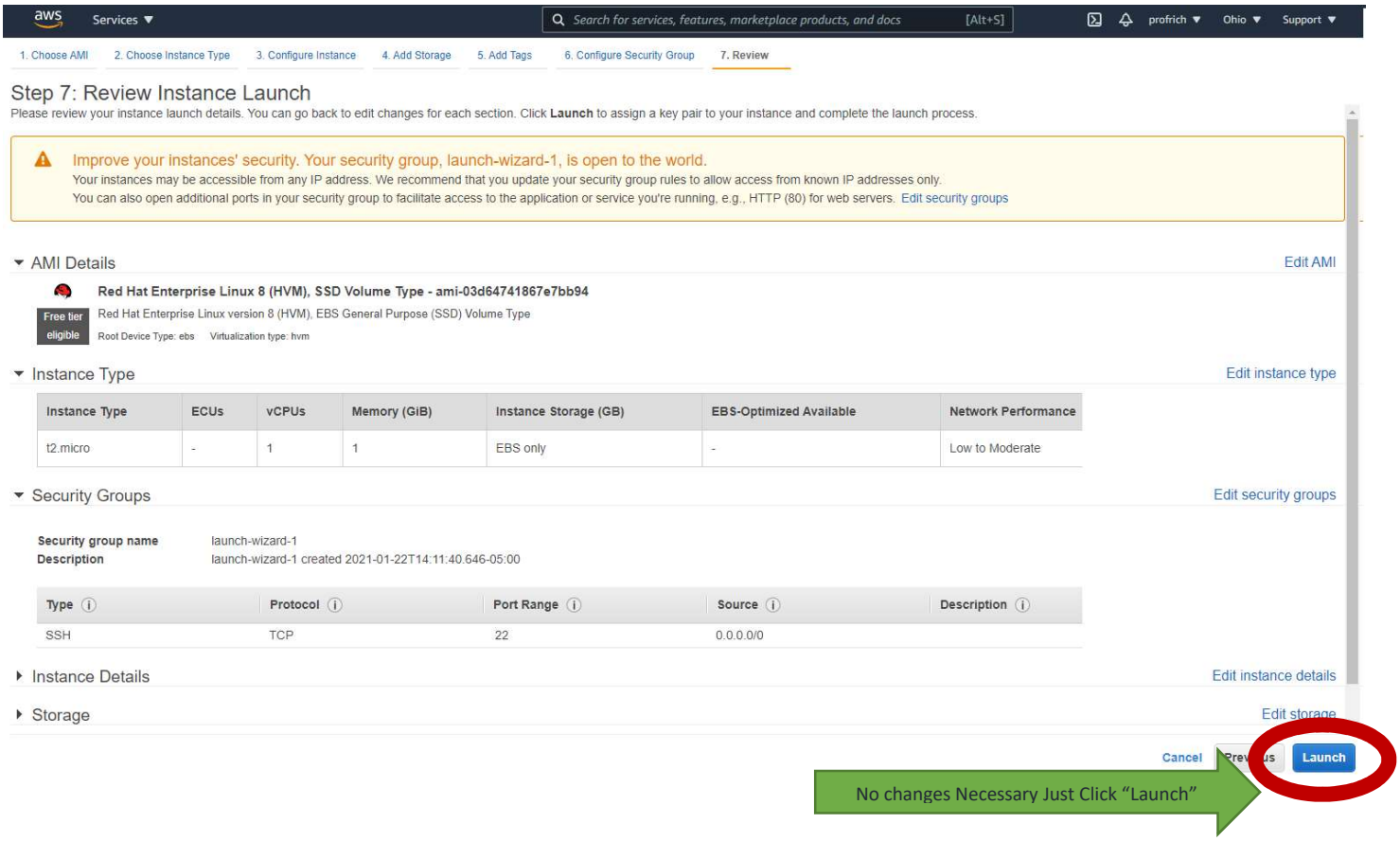
“Launch Instances”

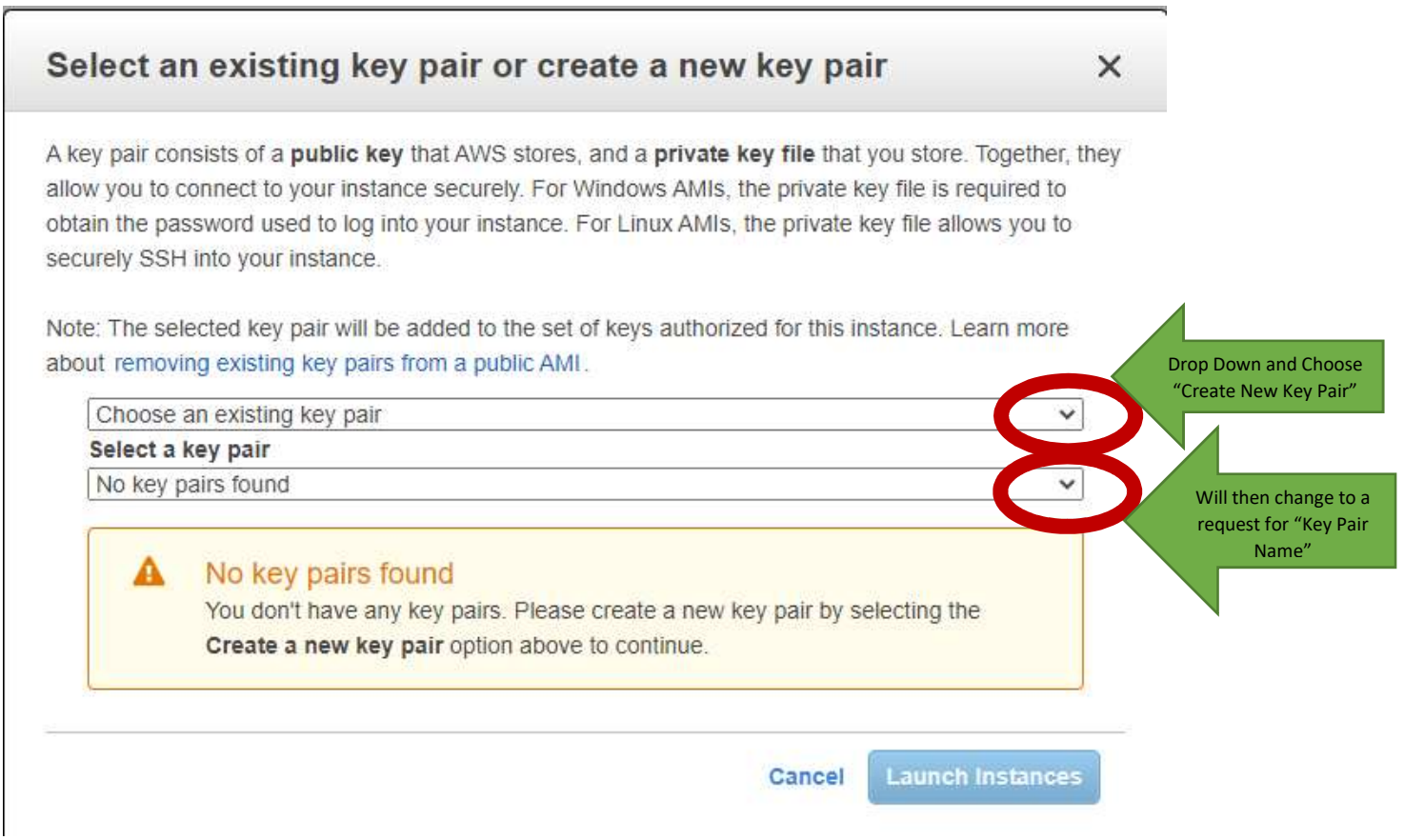


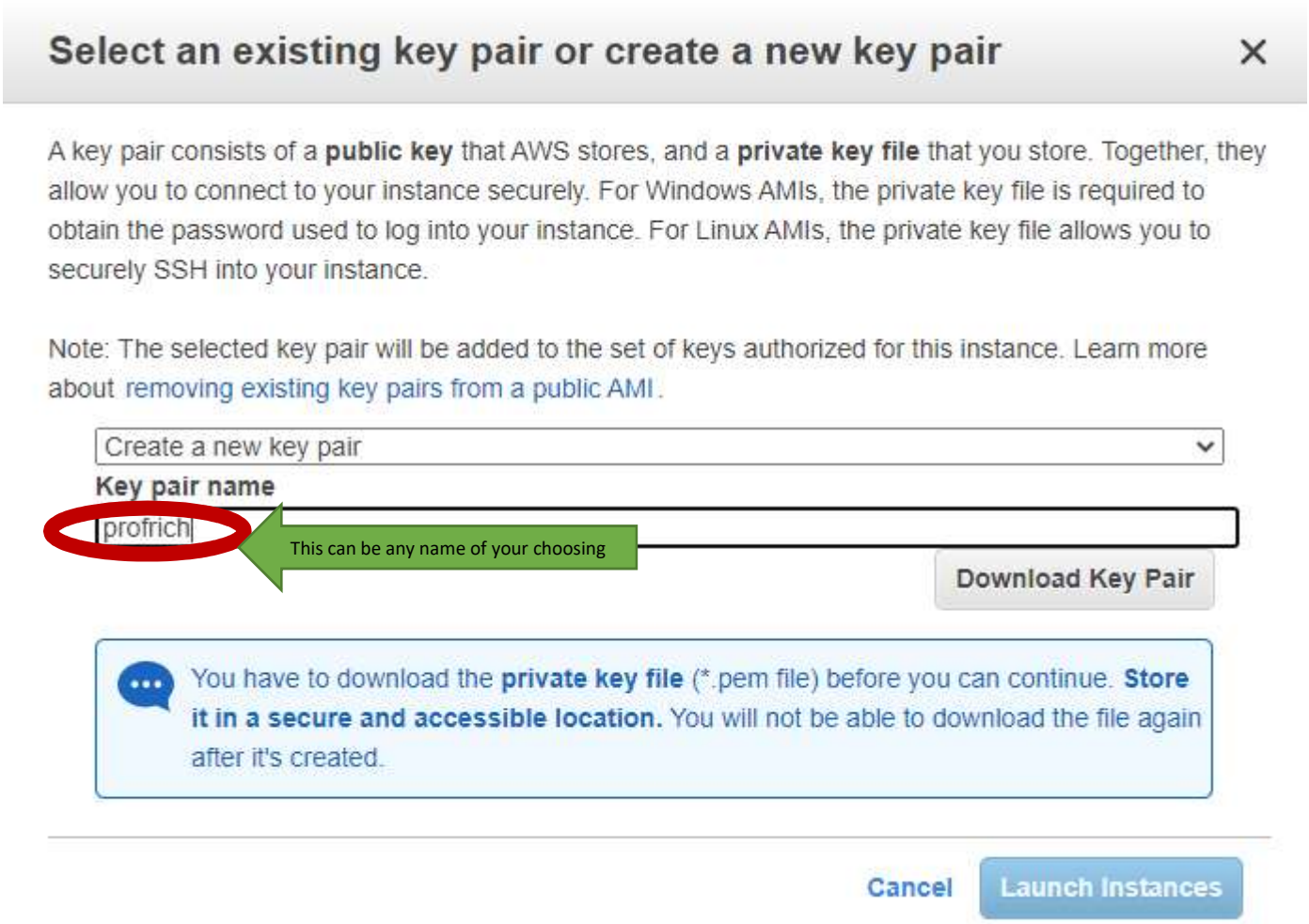




Double check to make sure that a "Free tier eligible" Type is chosen (the blue dot indicates chosen


aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
profrich
Ohio
Support
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
Improve your instances' security. Your security group, launch-wizard-1, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-03d64741867e7bb94
Free tier eligible
Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type
Root Device Type: ebs Virtualization type: hvm
Instance Type
Edit instance type
Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance
t2.micro | - | 1 | 1 | EBS only | - | Low to Moderate
Security Groups
Edit security groups
Security group name launch-wizard-1
Description launch-wizard-1 created 2021-01-22T14:11:40.646-05:00
Type | Protocol | Port Range | Source | Description
SSH | TCP | 22 | 0.0.0.0/0
Instance Details
Edit instance details
Storage
Edit storage
Cancel
Launch
No changes Necessary Just Click "Launch"


Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
No key pairs found
No key pairs found
You don't have any key pairs. Please create a new key pair by selecting the Create a new key pair option above to continue.
Cancel
Launch Instances
Drop Down and Choose "Create New Key Pair"
Will then change to a request for "Key Pair Name"

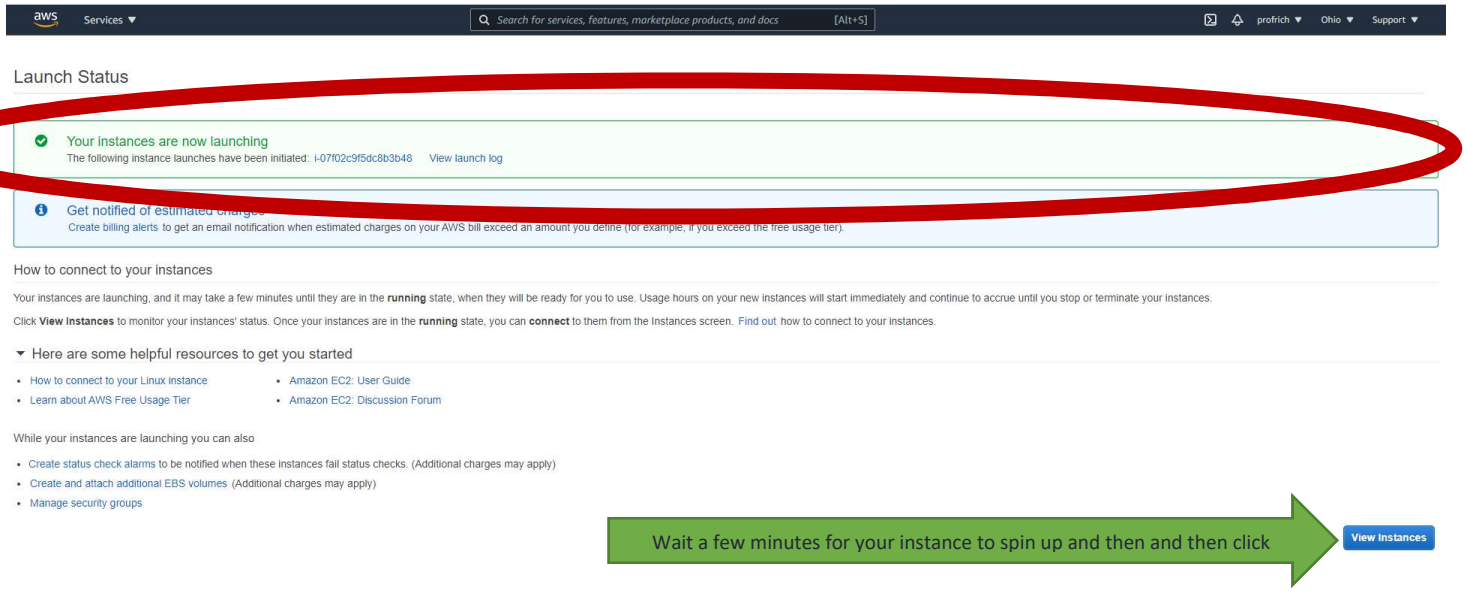


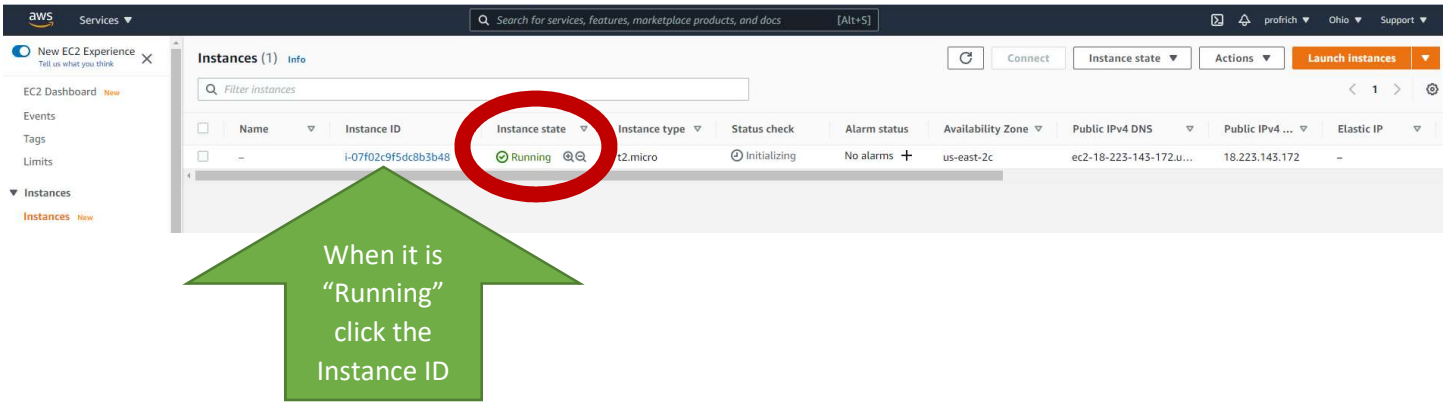
I chose the name of my key pair to be “profrich” (after my AWS account name)…you can name it whatever you would like. We will use this later.

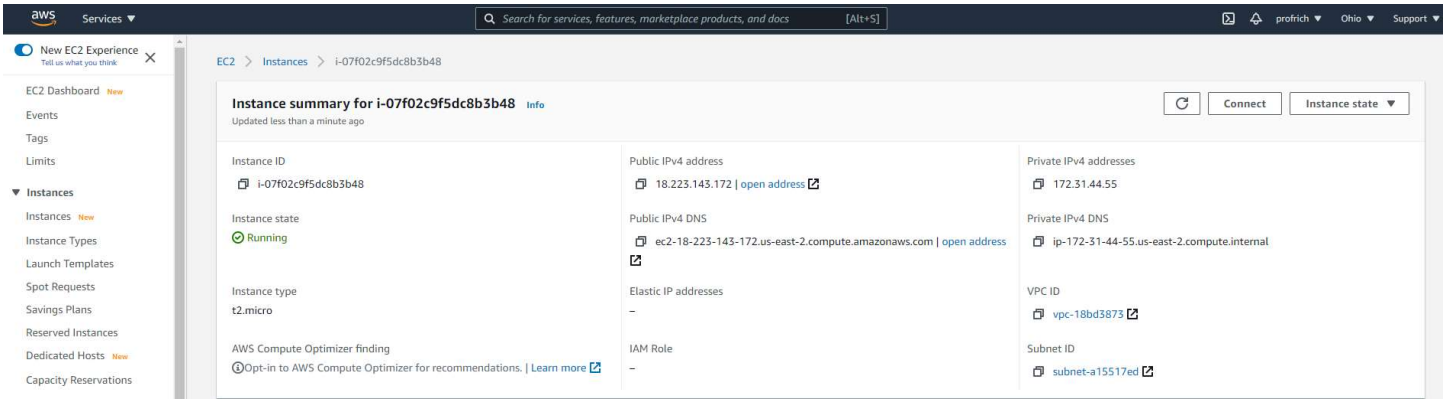
I received, in my download folder, a file called (in my case) “profrich.pem”

It is critical to **KEEP** in a **SECURE** place (preferably portable).

After downloading, the “Launch Instances” button will be available



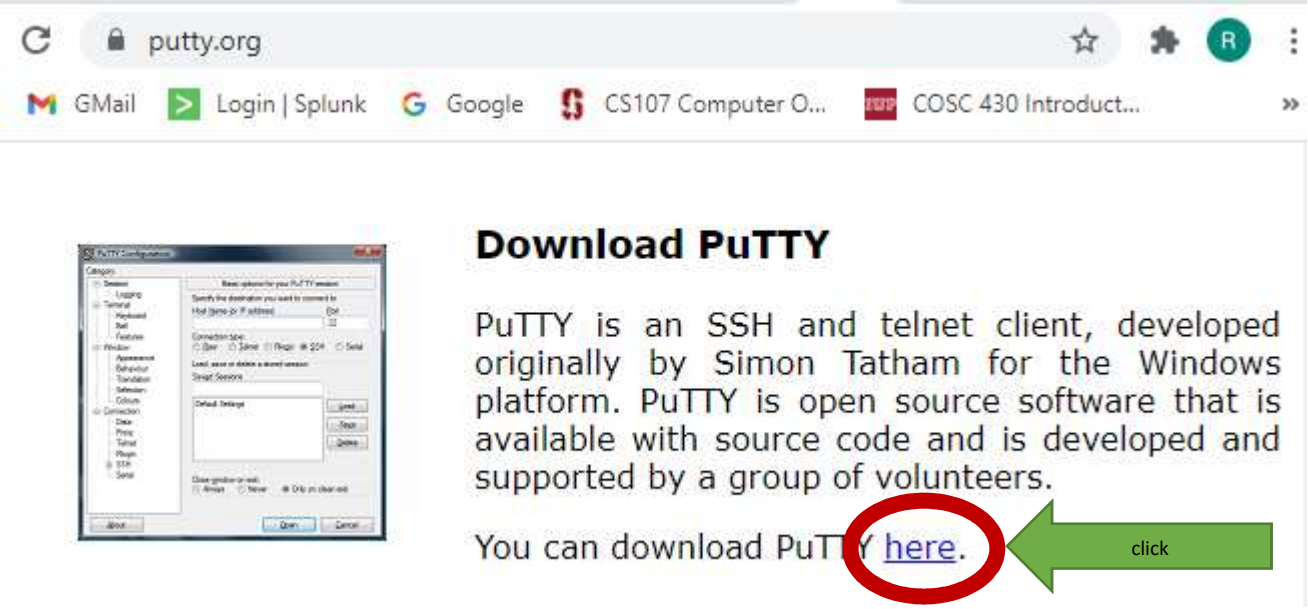




Your EC2 instance is now running,

- If you are using Windows, we will need PuTTY to connect to it. Just move onto the next page (page 8)
- If you are using a MAC, move onto page 17

Go to the site… https://putty.org/



Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel), but you can download standalone binaries one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)

32-bit:		(or by FTP)	(signature)
64-bit:	putty.exe	(or by FTP)	(signature)

pscp.exe (an SCP client, i.e. command-line secure file copy)

32-bit:	pscp.exe	(or by FTP)	(signature)
64-bit:	pscp.exe	(or by FTP)	(signature)

psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)

32-bit:	psftp.exe	(or by FTP)	(signature)
64-bit:	psftp.exe	(or by FTP)	(signature)

puttytel.exe (a Telnet-only client)

32-bit:	puttytel.exe	(or by FTP)	(signature)
64-bit:	puttytel.exe	(or by FTP)	(signature)

plink.exe (a command-line interface to the PuTTY back ends)

32-bit:	plink.exe	(or by FTP)	(signature)
64-bit:	plink.exe	(or by FTP)	(signature)

pageant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)

32-bit:	pageant.exe	(or by FTP)	(signature)
64-bit:	pageant.exe	(or by FTP)	(signature)

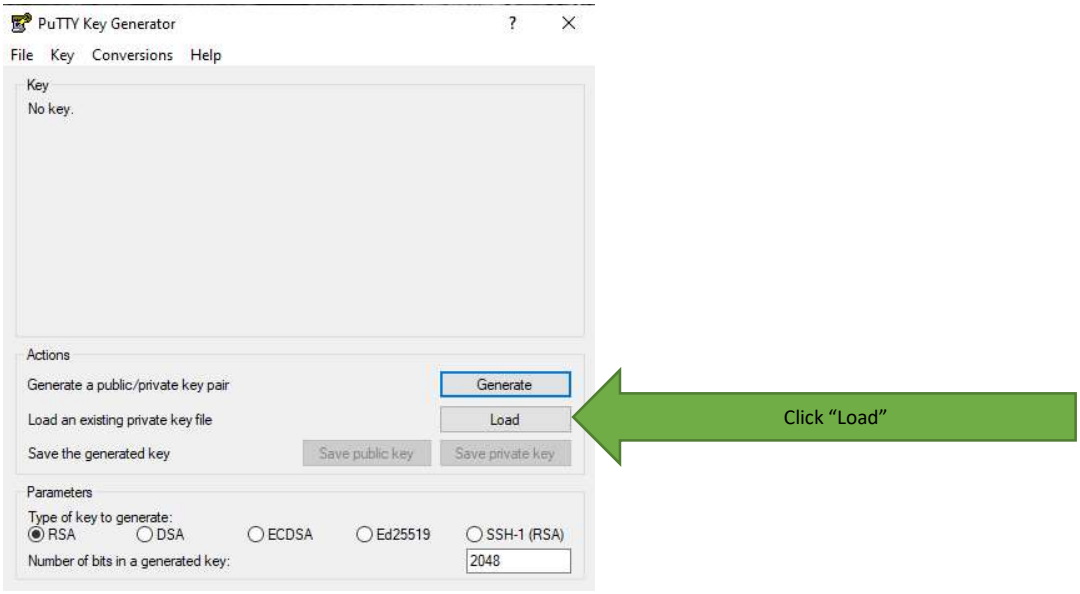
puttygen.exe (a RSA and DSA key generation utility)

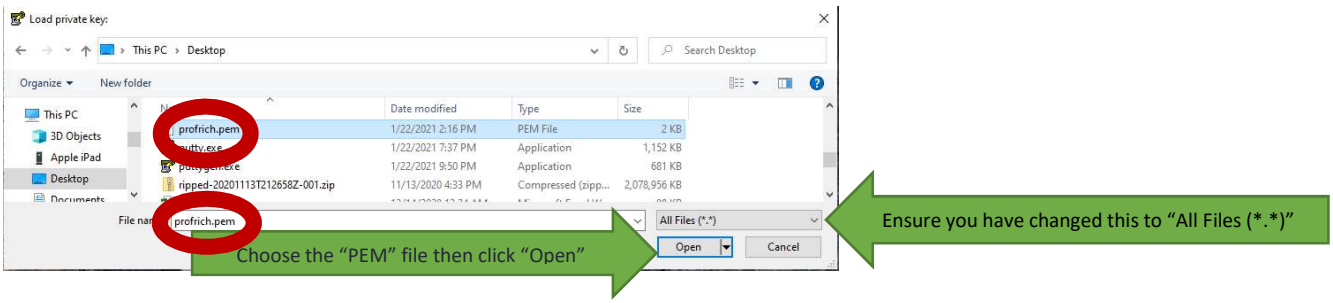
32-bit:		(or by FTP)	(signature)
64-bit:	puttygen.exe	(or by FTP)	(signature)

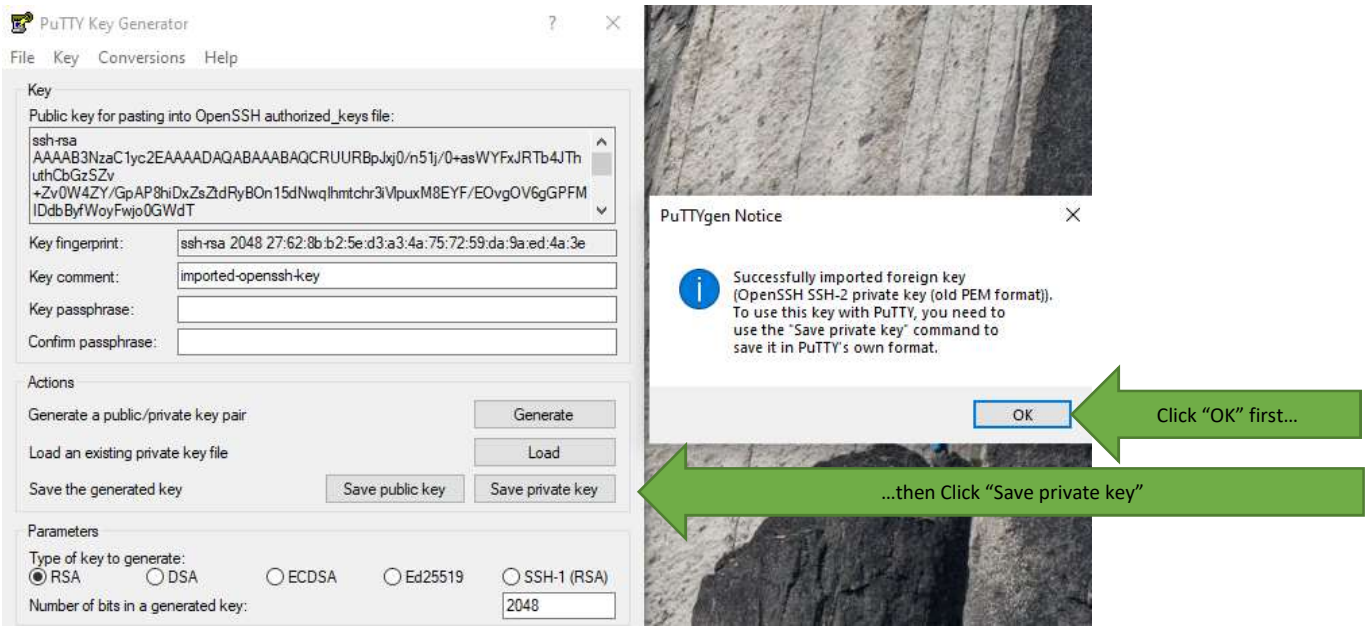
These are standalone files. Copy them from your download folder to your desktop

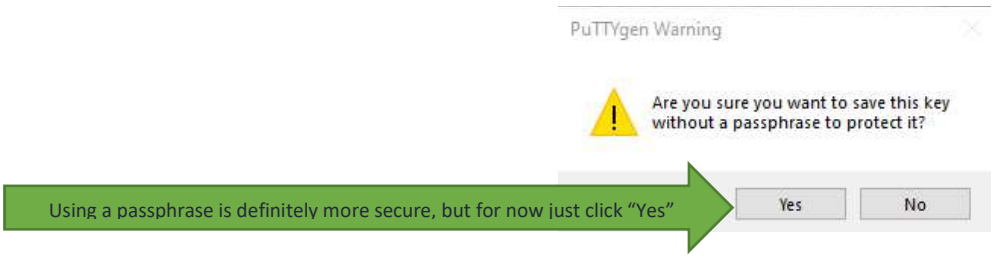
At this time you will also need your PEM file (mine was called “profrich.pem”). Please copy it from the download directory and move it to your desktop as well so you can find it. NOTE: if you prefer to put both of these in a folder it can be done at your discretion but just remember where they are)

Before we connect, we need to generate a key file based on that PEM file

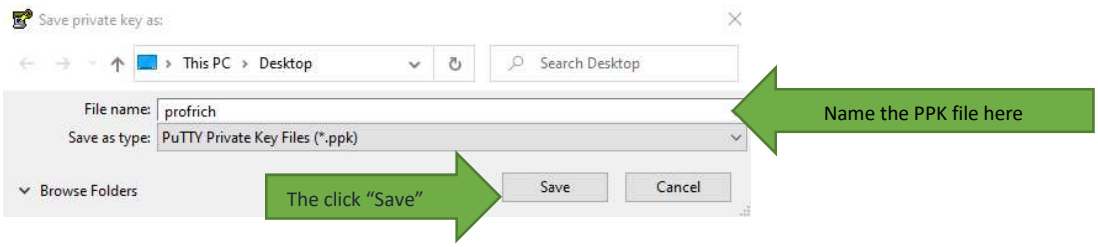


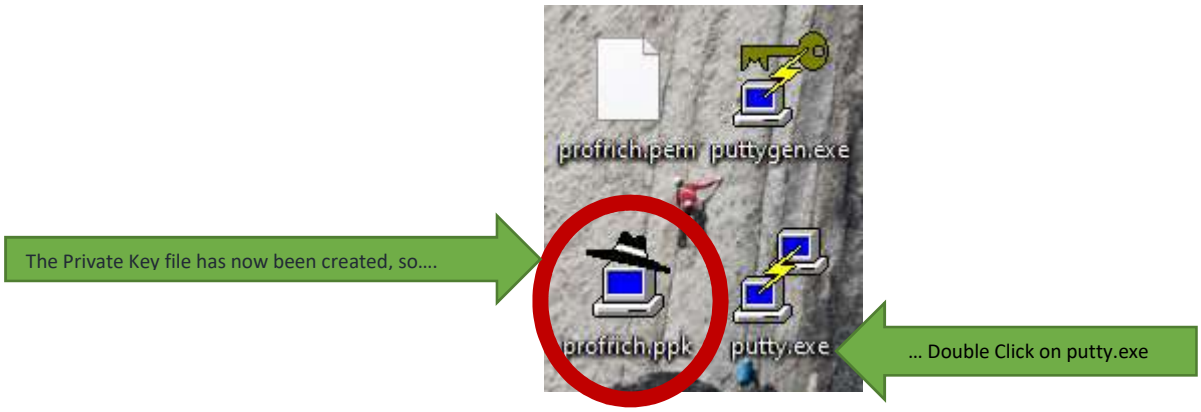


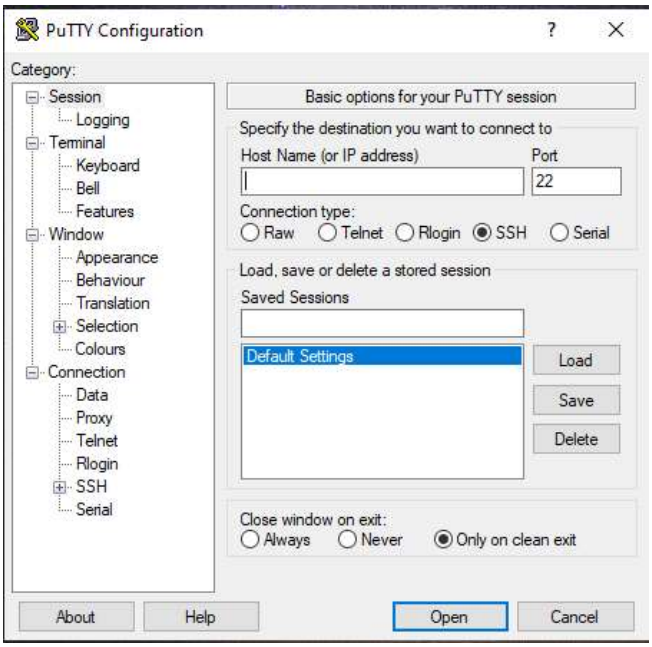




We will now save the private key file (which will have a “PPK” extension). Again, you can name this whatever you want, but you may want it to match your “PEM” file name. I did here…

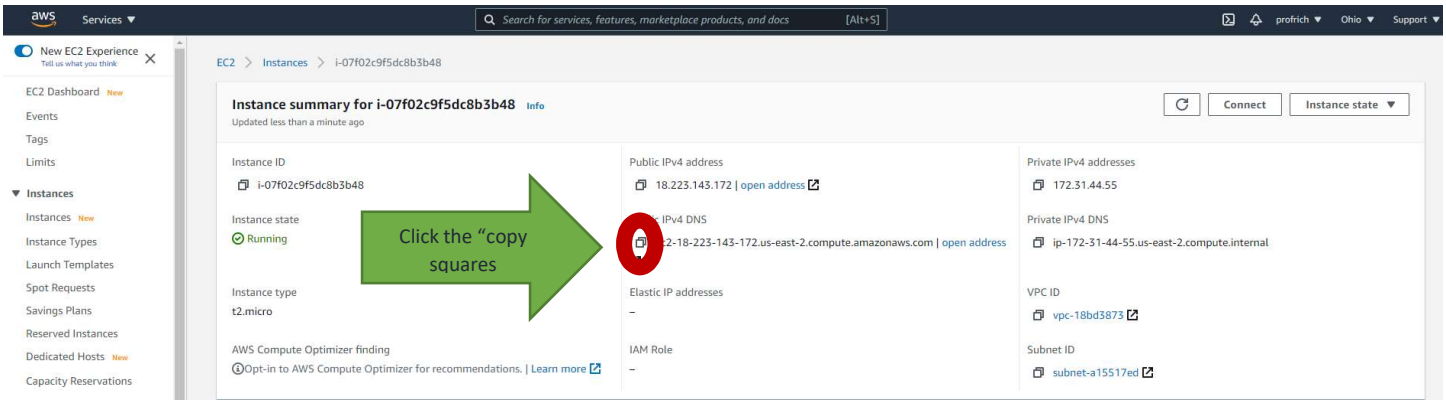


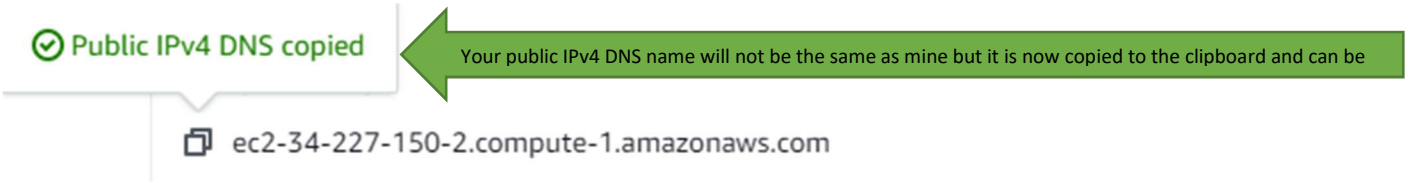




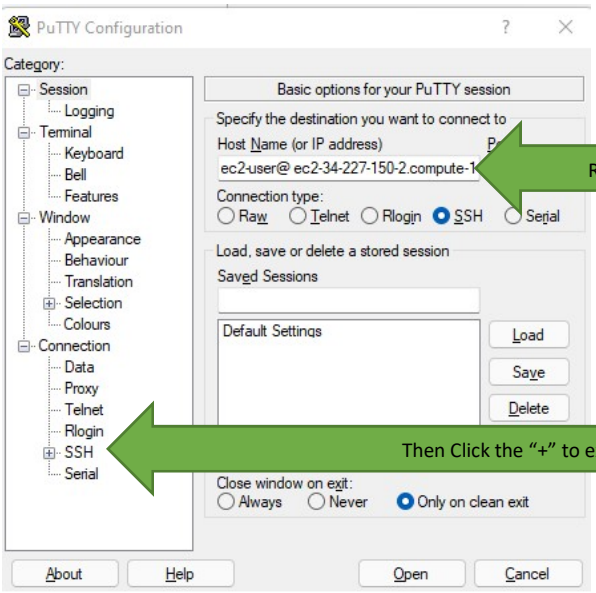
Don’t do anything yet!!! We must go back to our

Go back to your AWS console



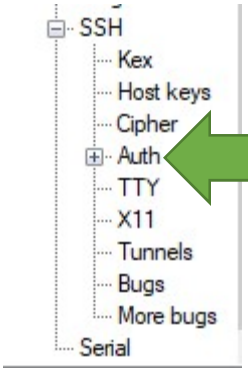


Go back to “PuTTY”

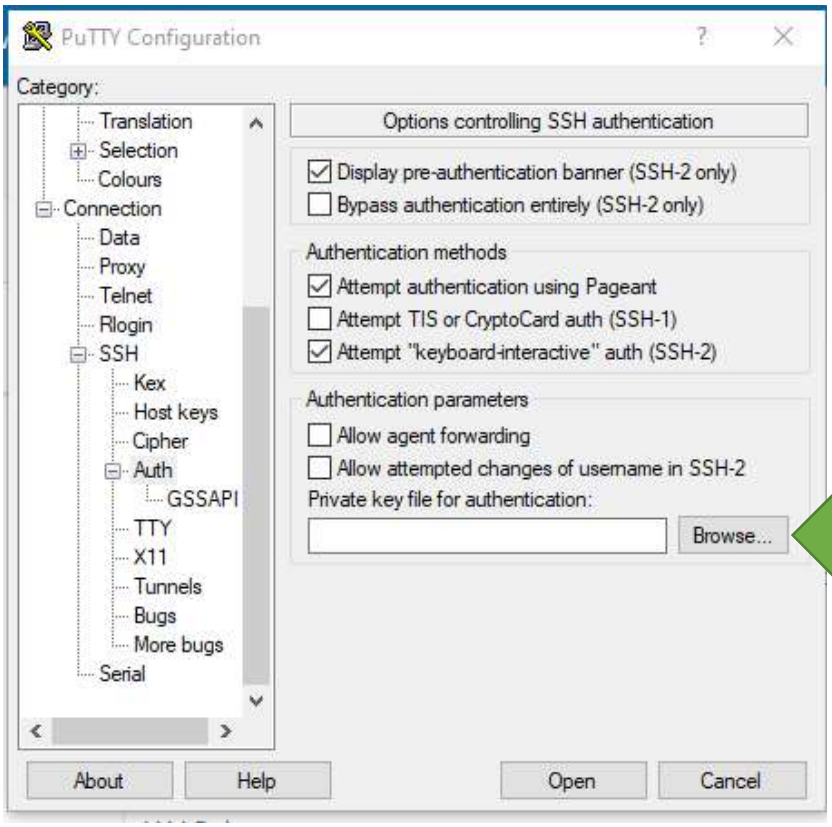


Right Click and paste the domain name of your EC2 prefixed by "ec2-user@"

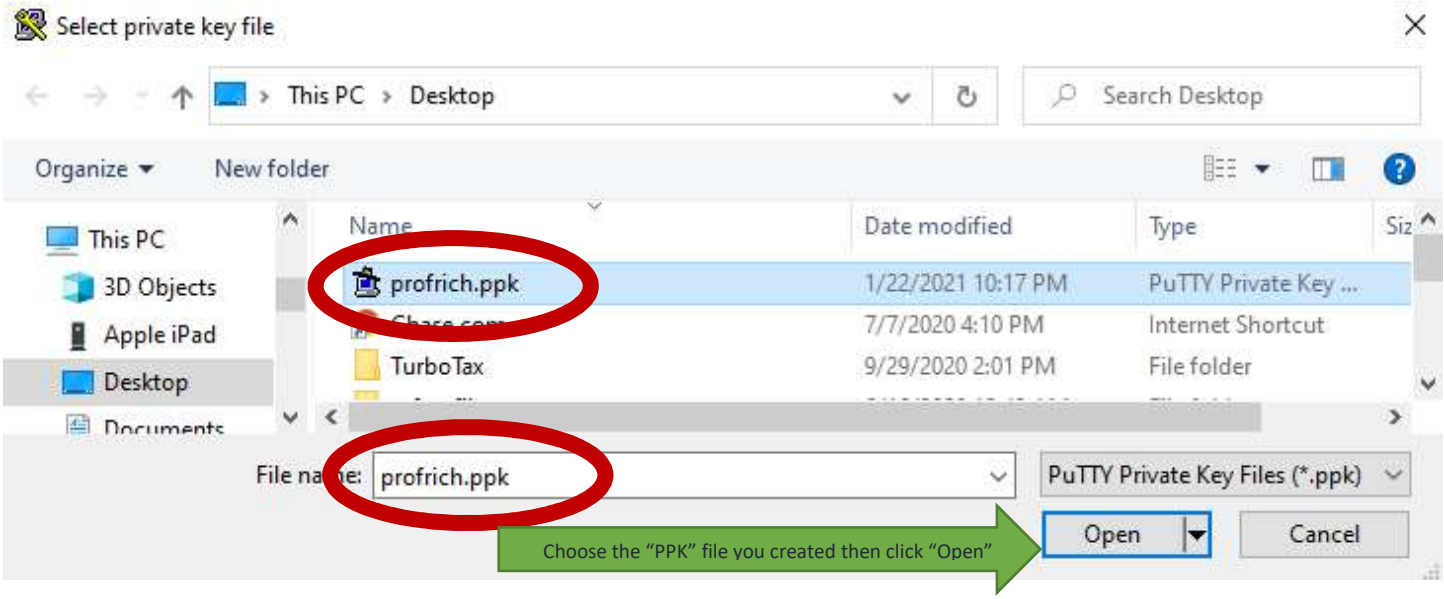
Then Click the "+" to expand "SSH"

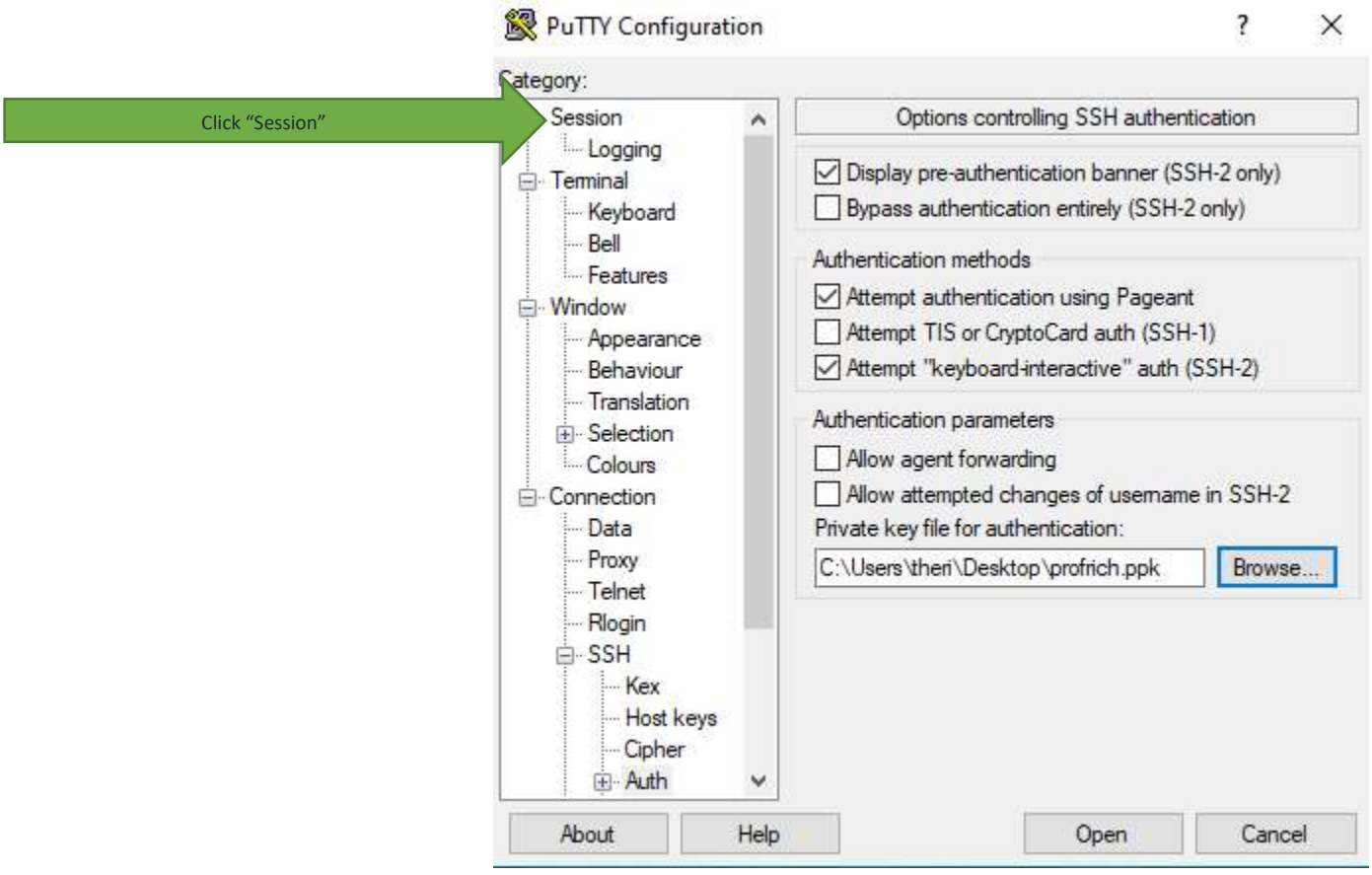


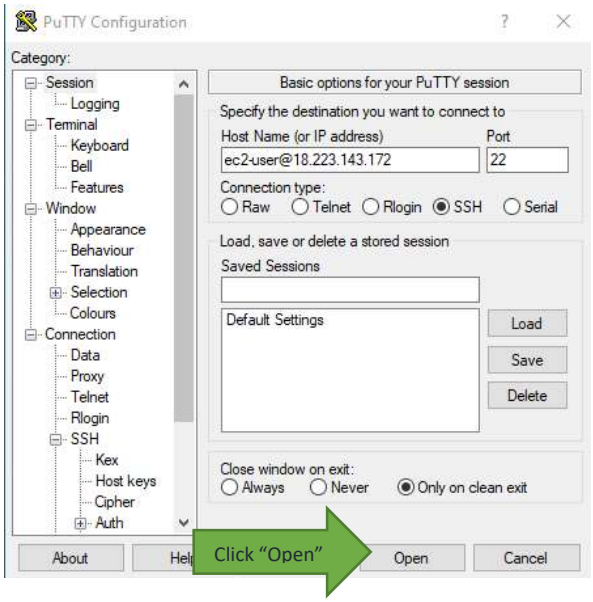
Then Click "Auth" (NOT the +)



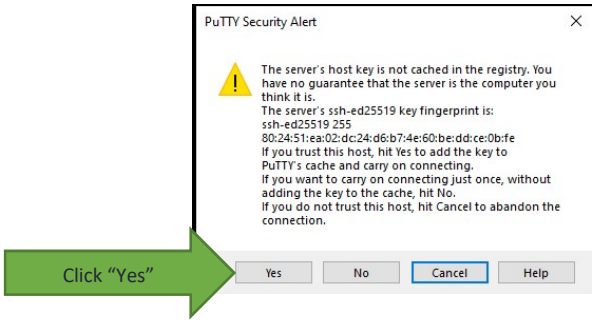
Click Browse and pick your PPK file


Select private key file
This PC › Desktop
Search Desktop
Organize
New folder
This PC
3D Objects
Apple iPad
Desktop
Documents
Name
Date modified
Type
profrich.ppk
1/22/2021 10:17 PM
PuTTY Private Key ...
7/7/2020 4:10 PM
Internet Shortcut
TurboTax
9/29/2020 2:01 PM
File folder
File name:
profrich.ppk
PuTTY Private Key Files (*.ppk)
Choose the "PPK" file you created then click "Open"
Open
Cancel

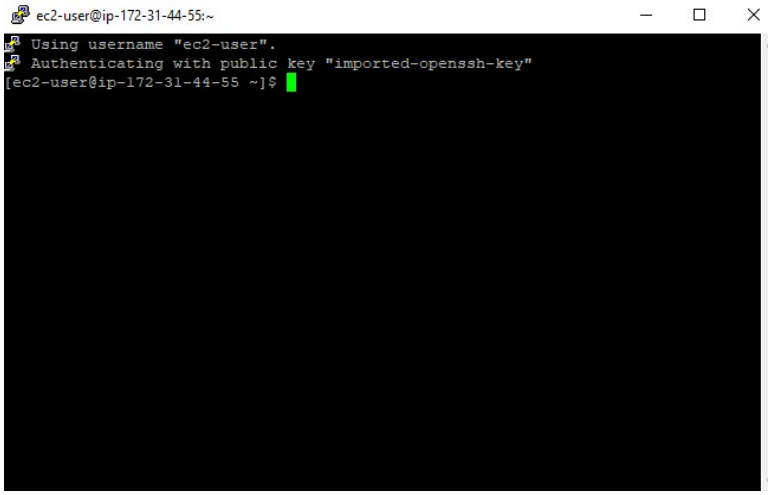

Click "Session"
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Host keys
Cipher
Auth
Options controlling SSH authentication
Display pre-authentication banner (SSH-2 only)
Bypass authentication entirely (SSH-2 only)
Authentication methods
Attempt authentication using Pageant
Attempt TIS or CryptoCard auth (SSH-1)
Attempt "keyboard-interactive" auth (SSH-2)
Authentication parameters
Allow agent forwarding
Allow attempted changes of username in SSH-2
Private key file for authentication:
C:\Users\theri\Desktop\profrich.ppk
Browse...
About
Help
Open
Cancel



NOTE: Here you can also assign a name under “Saved Sessions” and save your settings for later use by then hitting “Save”



SUCCESS!!!



When you are done with your work every day, please don’t forget to shut down your EC2.

If you leave it up you will eventually be charged!!!

Go to page 16 for instructions

IMPORTANT NOTES!!!!

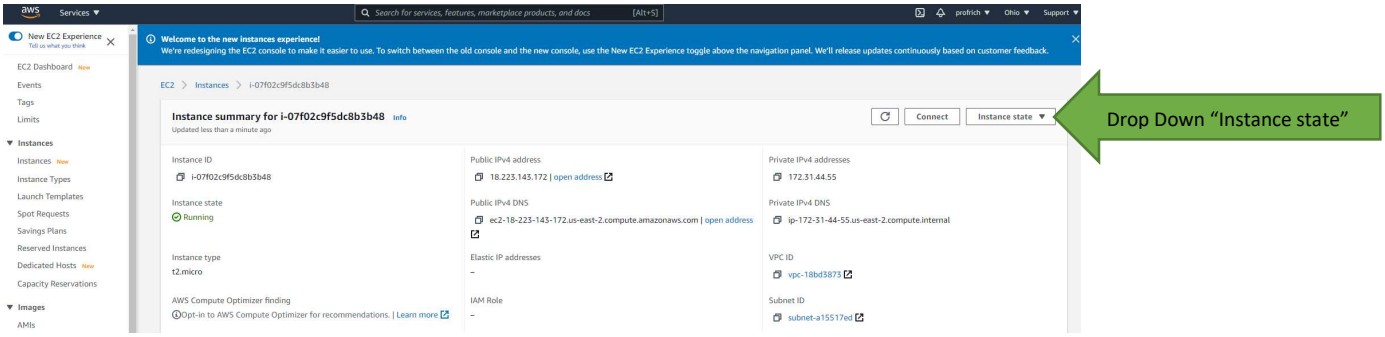
1. Macs do not use PuTTY. Use the page of this document to dedicated to explaining connecting using a MAC. Do not do any of the instructions referring to “putty.exe” nor “puttygen.exe” on the following pages.

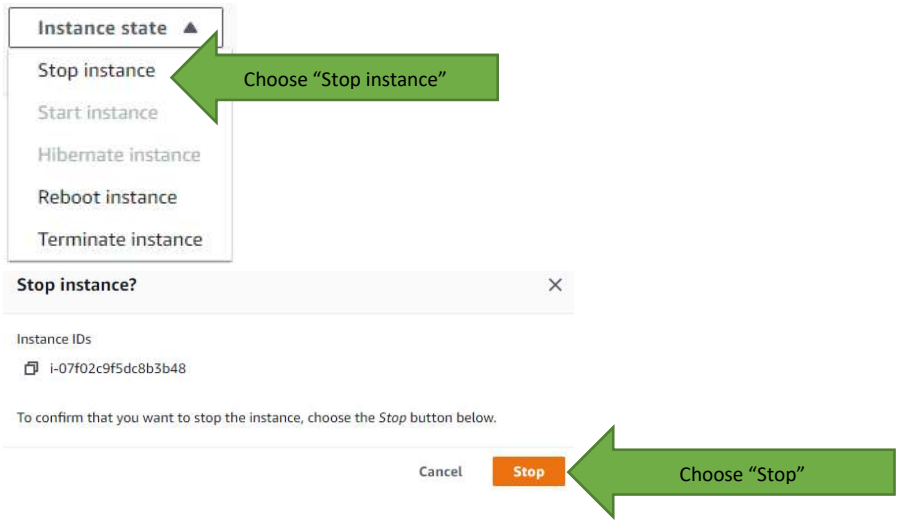
2. **Please save your PEM and PPK file somewhere portable, like in your e-mail**. When you are on campus it can be shared to your network drive, but for now a good way to make sure you always have these files is to mail them to yourself. NOTE: this is NOT a good idea normally due to security, but we are in an academic environment with ephemeral resources. DO NOT do this in a professional environment…a KEY (PPK) file should always be stored and transferred encrypted and secure!!!

3. To close your PuTTY session you can just click the “x” in the upper corner or just type “exit”

4. DO NOT leave your EC2 running. If you do, they WILL begin to charge you for its use even before the 12 months they promised. Please see the section regarding “Shutting down your EC2”

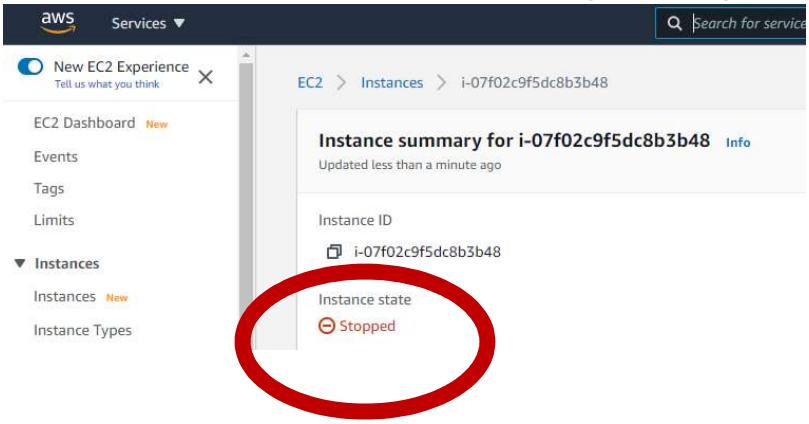
Shutting Down your EC2





Look for this message…

But don’t believe it…keep refreshing the page until you see…



If it does not stop, try stopping it again until it does stop.

Macs

Please create your EC2 as instructed, but once you have downloaded your PEM file and have recorded the public IPv4 Domain Name of your new EC2, you can connect by doing the following…

1. Run your terminal app
2. In your home directory run the command "*cd .ssh*"

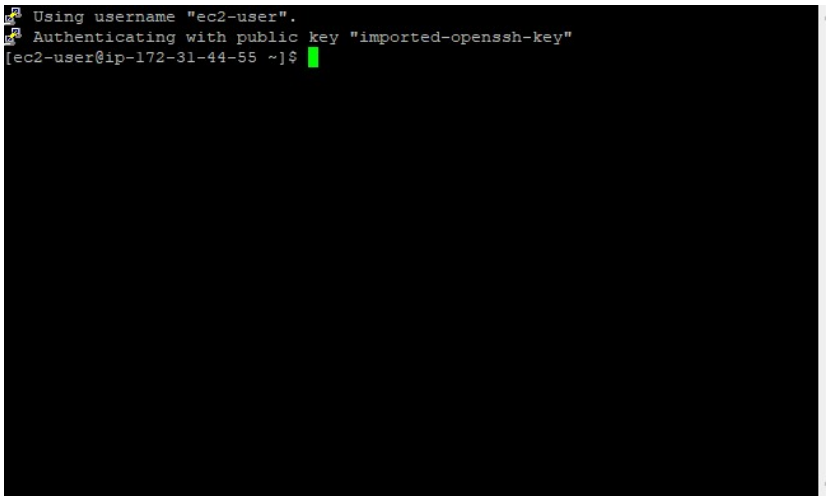
   if you get an error run "*md .ssh*" , then "*cd .ssh*"
3. Copy the PEM file you downloaded when you created your EC2 instance to that directory.
4. Run the command "*chmod 400 nameofyourfile.pem*"

   PLEASE REPLACE "nameofyourpemfile" with its actual name!!!!
5. You can now connect to your EC2 using the command

   "ssh -i nameofyourpemfile.pem ec2-user@yourEC2sDomainName"

   WHERE "yourEC2sDomainName" is the "Public IPv4 Domain Name of your EC2"

SUCCESS!!!



When you are done with your work every day, please don't forget to shut down your EC2.

If you leave it up you will eventually be charged!!!