Clone CS5910 AWS EC2 Instance

In this lesson, we show how to create AWS EC2 Instance using Platform as a Service from AWS. We follow the workflow of seven-step process to configure the instance. We will create a t2.micro (free tier) instance with default 8GB elastic storage.
We also choose VPN private LAN for its network connectivity so that it is protected by default. We will configure its security group (firewall) with SSH, HTTP, and HTTPS services open and only allow your local machine to access by specifying the IP address of the local machine as the only source to connect. At the last step of the configuration, be sure to create the public/private key pair for accessing your customized Linux machine and download the private key in .PEM file format. Backup the private key in some safe place. Once you lost the private key you cannot the Linux machine again.

Let us first login to AWS management console.
After login to AWS management console, click the second upper right tab to see the list of regions available on AWS and select the region where you will create your instance. Typically, this is the region closer to you or to your customers. In our case, pick the one closer to you, since this will be the instance for your cyber security study and it is better to be responsive!!
If it is not clear to you which region is closest to you, you can follow the procedure in http://ciast.uccs.edu/coursera/pub/PickClosestAWSRegion.pdf and pick the region based on the ping results.

Note that the AWS remembers which region you last access.
After choosing the region, click the ec2 service on the left. See Figure 1.

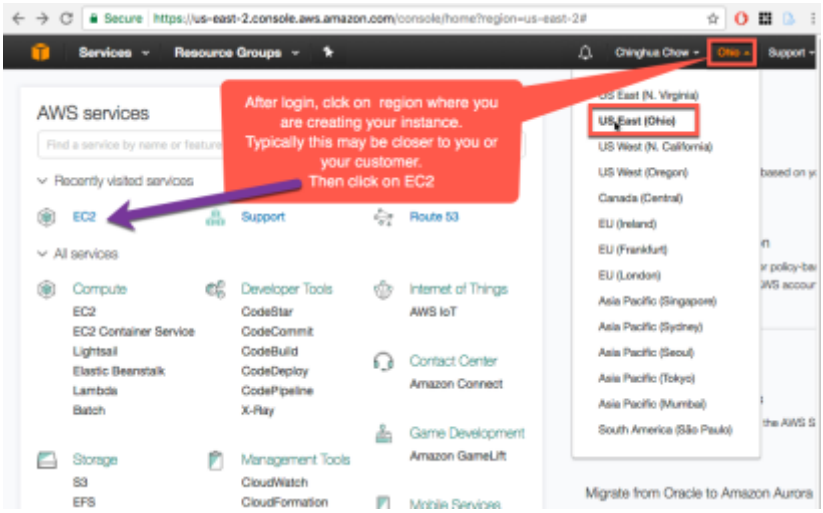


Figure 1. Select Region and Start EC2 GUI.

We are presented with EC2 tool windows. The right side is EC2 dashboard, where the key resources such as current instances can be clicked and accessed. The Images section contains public and private images for cloning the instances. The snapshots can also be accessed there.

The network & Security shows the Security Groups, Elastic IPs, KeyPairs. The middle canvas window shows the current statistics of resources available in our account.
Click “Launch Instance” to create a new EC2 instance. See Figure 2.

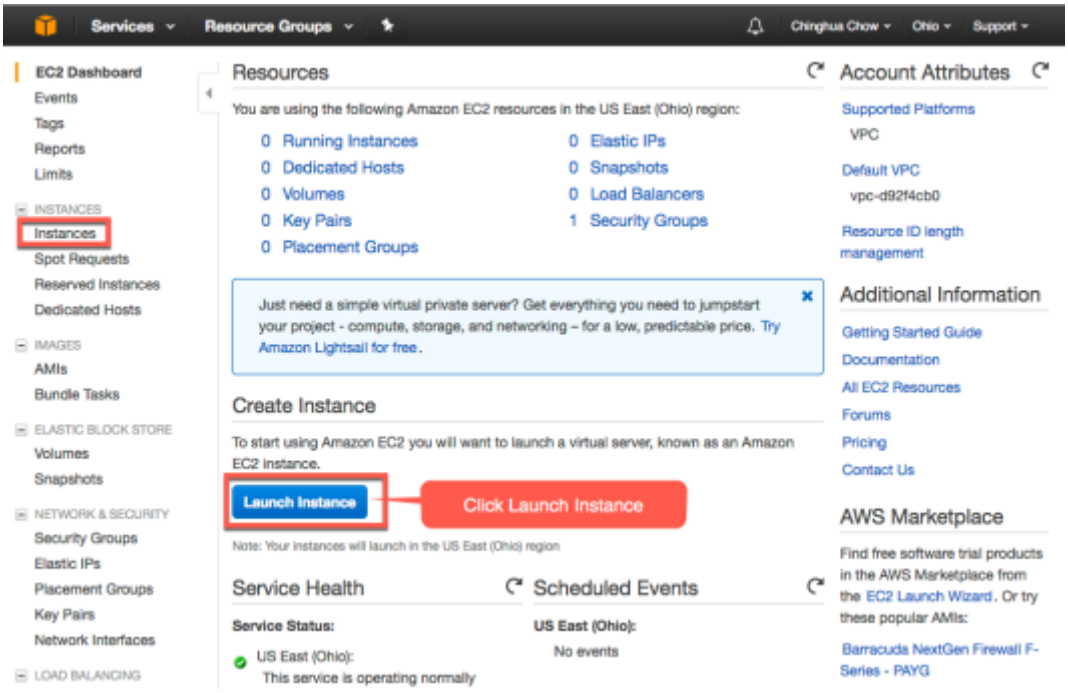


Figure 2. EC2 resources and Launch Instance.

Step 1. Choose an Amazon Machine Image (AMI)
Here we pick the AMI image I created from an instance and make it public for the community. The name of the AMI image is Coursera-CS591-AMI2. Therefore I select the “Community AMIs under My AMIs menu. Enter the “Coursera” in the query box to search for the AMI image. Click the image with name Coursera-CS591-AMI2. See Figure 3.

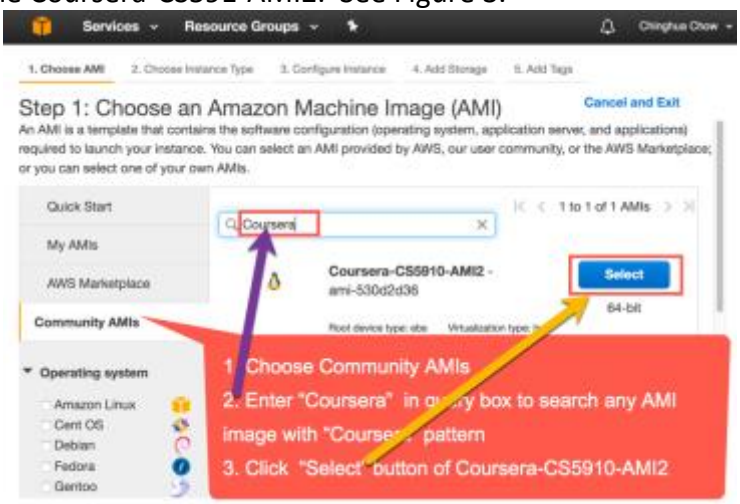


Figure 3. Step 1. Choose AMI Image.

Step 2. Choose an instance Type.
Here we choose the default t2.micro, a free tier computing resource.
Then choose "Next: Configure Instance Details. Do not choose default "Review and Launch", since we would like to add tag to this instance and configure its security group. See Figure 4.

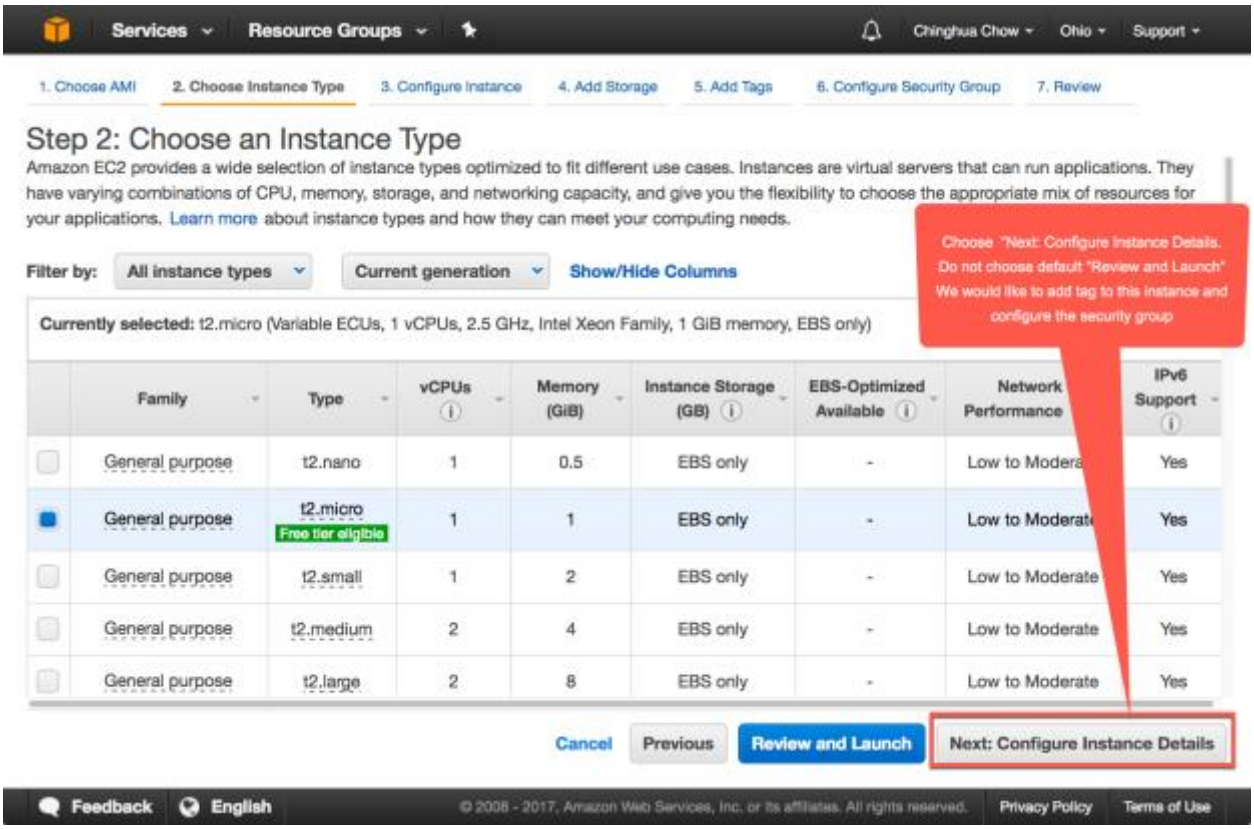


Figure 4. Choose instance type.

Step 3. Configure Instance details.
We can choose to put the instance on a specific subnet on one of the available zones.
e.g. here we chose the default zone us-east-2c. See Figure 5a. Note that if we open the advanced details section, there is a User data textbox. We can enter self-configured script for installing specific pkgs on the instance. The script will be executed once the instance is started.
Click Next Add Storage.

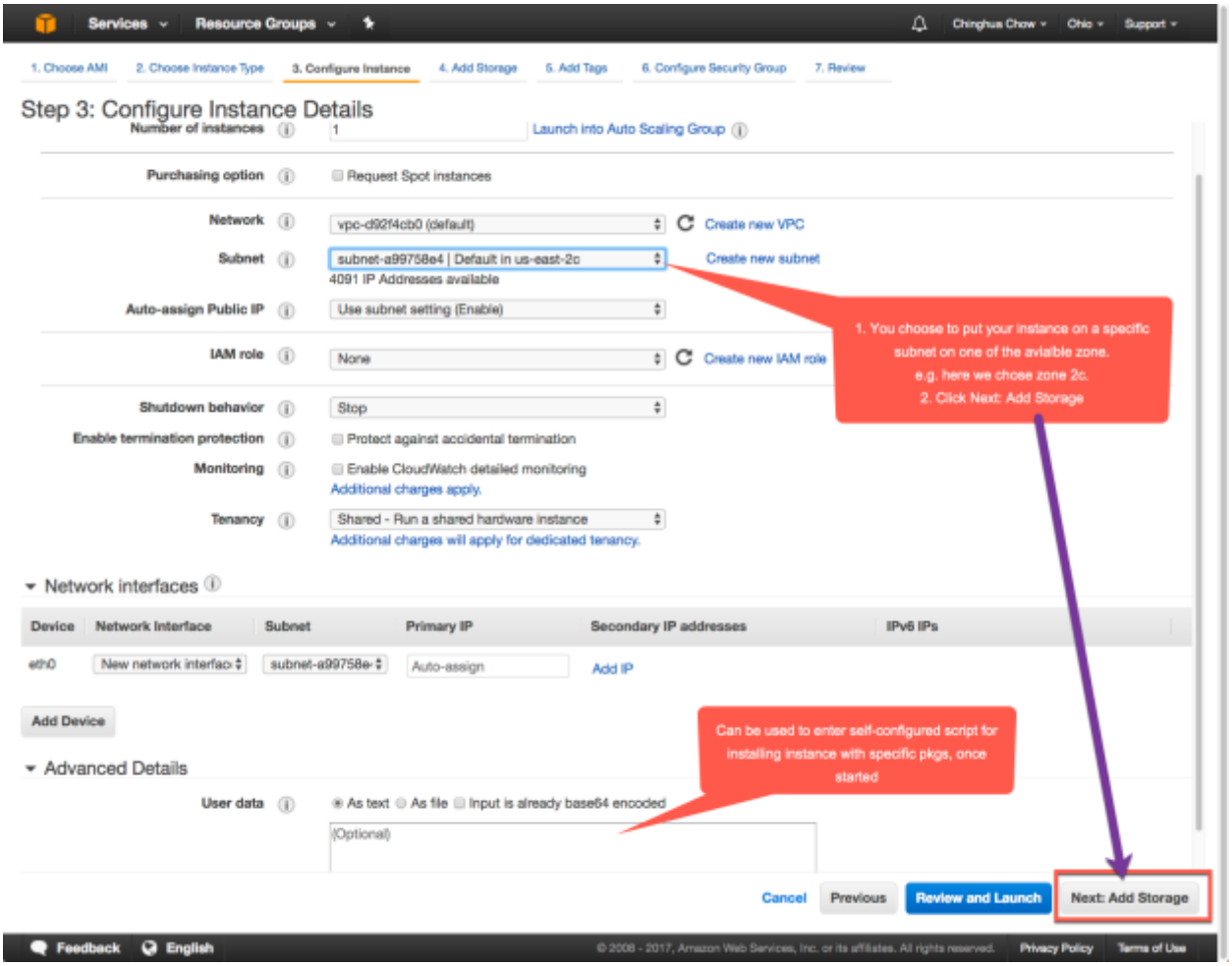


Figure 5a. Choose instance details, including choosing availability zones, add interfaces.

Choosing Availability Zone to host the instance.

Figure 5b shows that in the drop down menu for subnet, we see there are 3 different subnets, (us-east-2a, us-east-2b. and us-east-2c) in different availability zones of us-east-2 (Ohio Region). The availability zones are located in the same region but not at the same building or campus. In case there are natural or man-made disasters such as earth quake, cyber attacks, or fire to one available zone, others may not be affected. Setting up two instances with the same image on different availability zones or different regions increase the availability of the system.

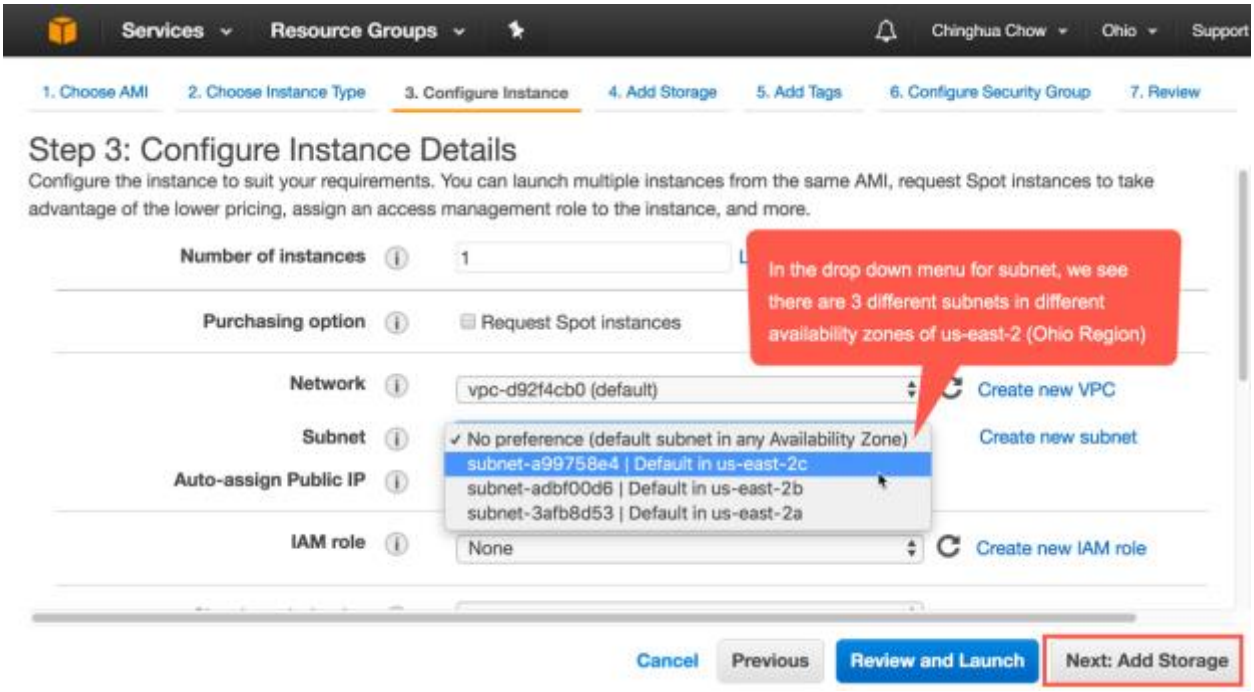


Figure 5b. Choose availability zones within a region to host the instance

Step 4. Add storage.

Choose default here, unless you like to increase the ELB (Elastic Block) storage. Normally 8 GB is enough storage to contain patches and for run simple cyber security exercises and web apps. You can also add a storage volume, such as shared disk. Click Next: Add Tags. See Figure 6.

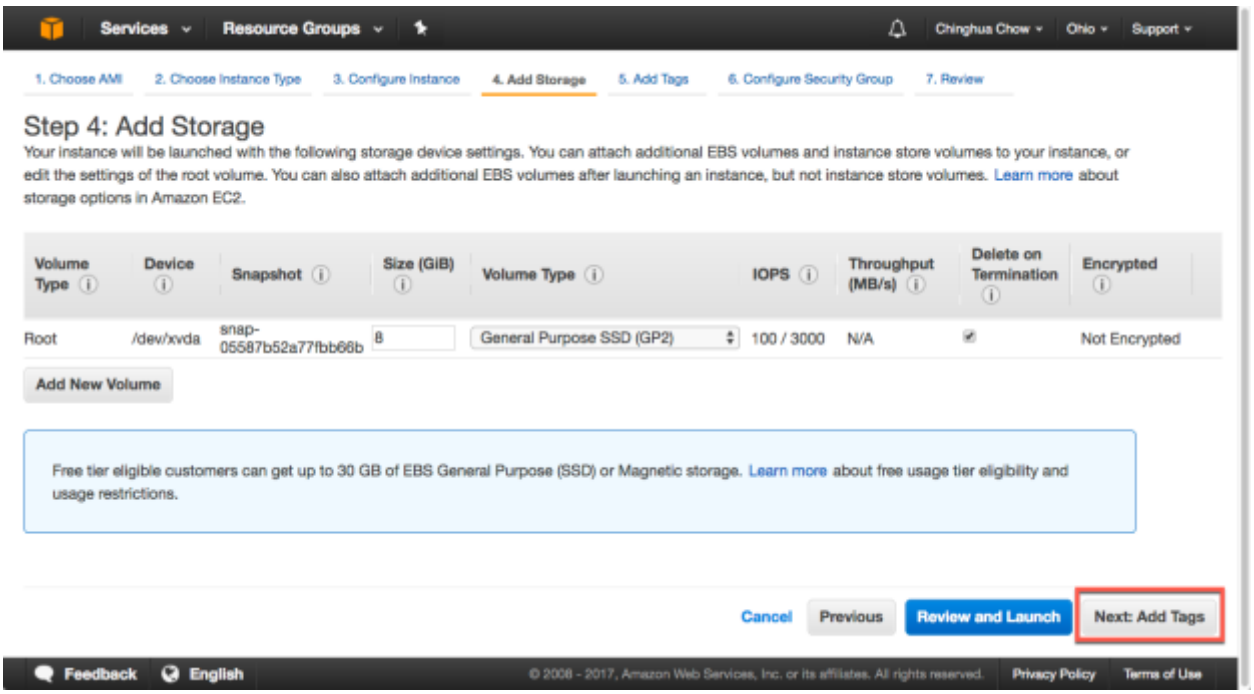


Figure 6. Add storage.

Step 5. Add tags.
Here we add two tags. ”Name” with capital N as key and Type as key. The Name tag will be listed as a column with the instances in EC2 main canvas windows. Make it easier to distinguish them for management purpose. Especially when you have many similar instances, such as my cloud or security class where all students are creating similar instances or clone the same image. It is useful to use <yourEmailAddress>_AMILinux_i<number> format as tag to tell them apart. Here I enter cchow@uccs.edu_AMILinux_i1 so that my students know this instance belong to me. Then click Next: Configure Security Group. See Figure 7.

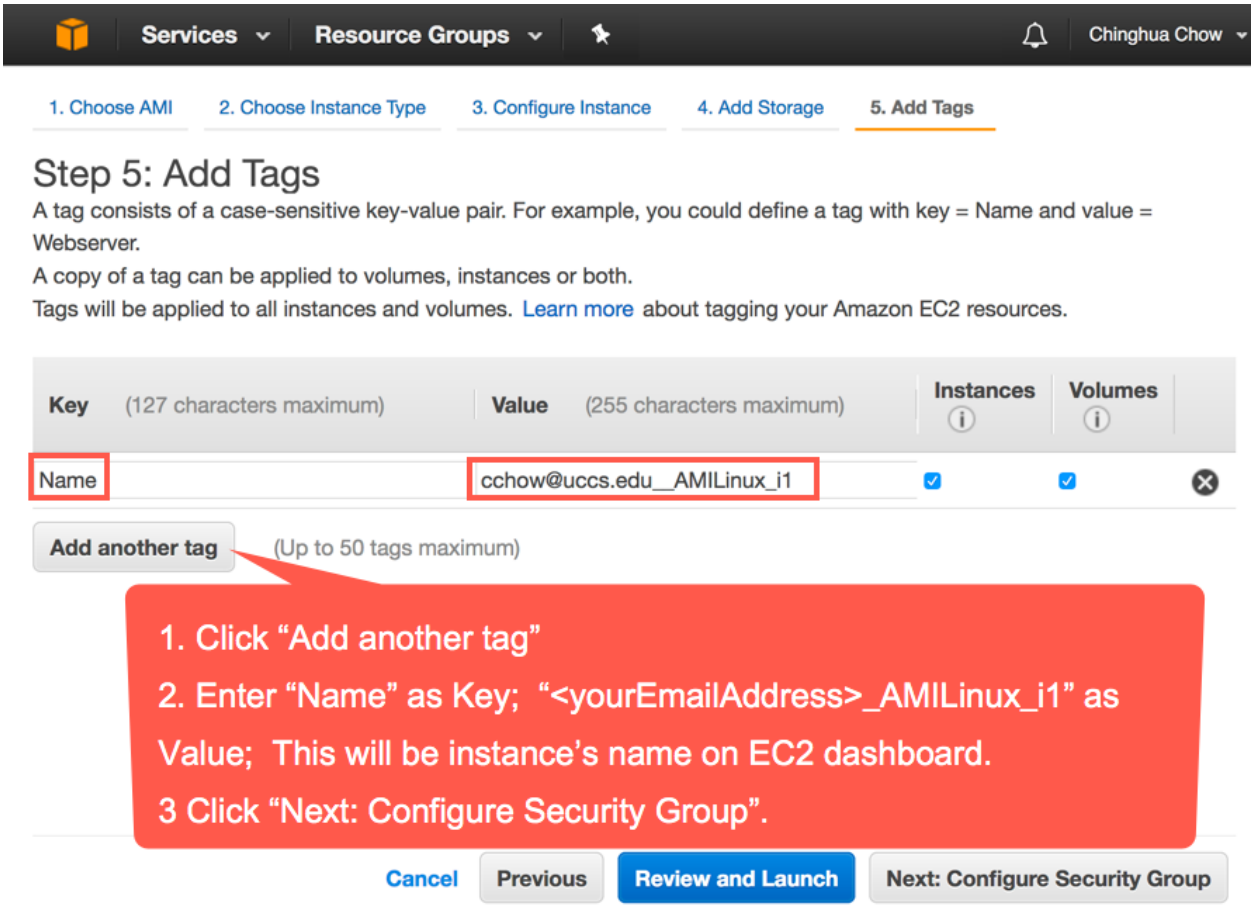


Figure 7. Add tag to identify the instance.

Step 6. Configure Security Group.
Click “Add Rule” twice I add two firewall rules. I then use the drop down menu to choose HTTP and HTTPS for those two rules. I then enter myip in google search box to find my home IP address, 118.166.240.100. See Figure 8.

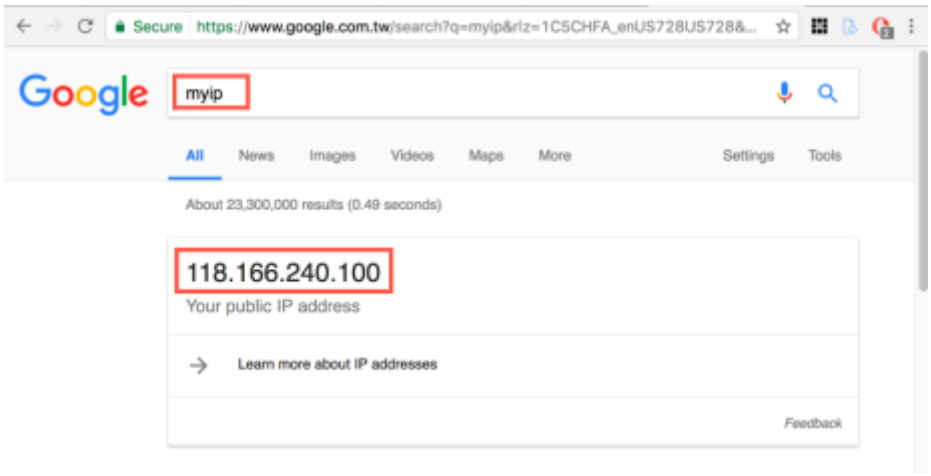


Figure 8. Finding the IP address of my local machine.

Enter it with /32 in all source entries. This setting restricts the access of the instance and only allow access from my machine at home. It is critical that we protect this infant instance, since it is not yet patched and we do not want a hacker to invade it! We can later relax the access restriction once it is patched. Click Review and Launch. See Figure 9.

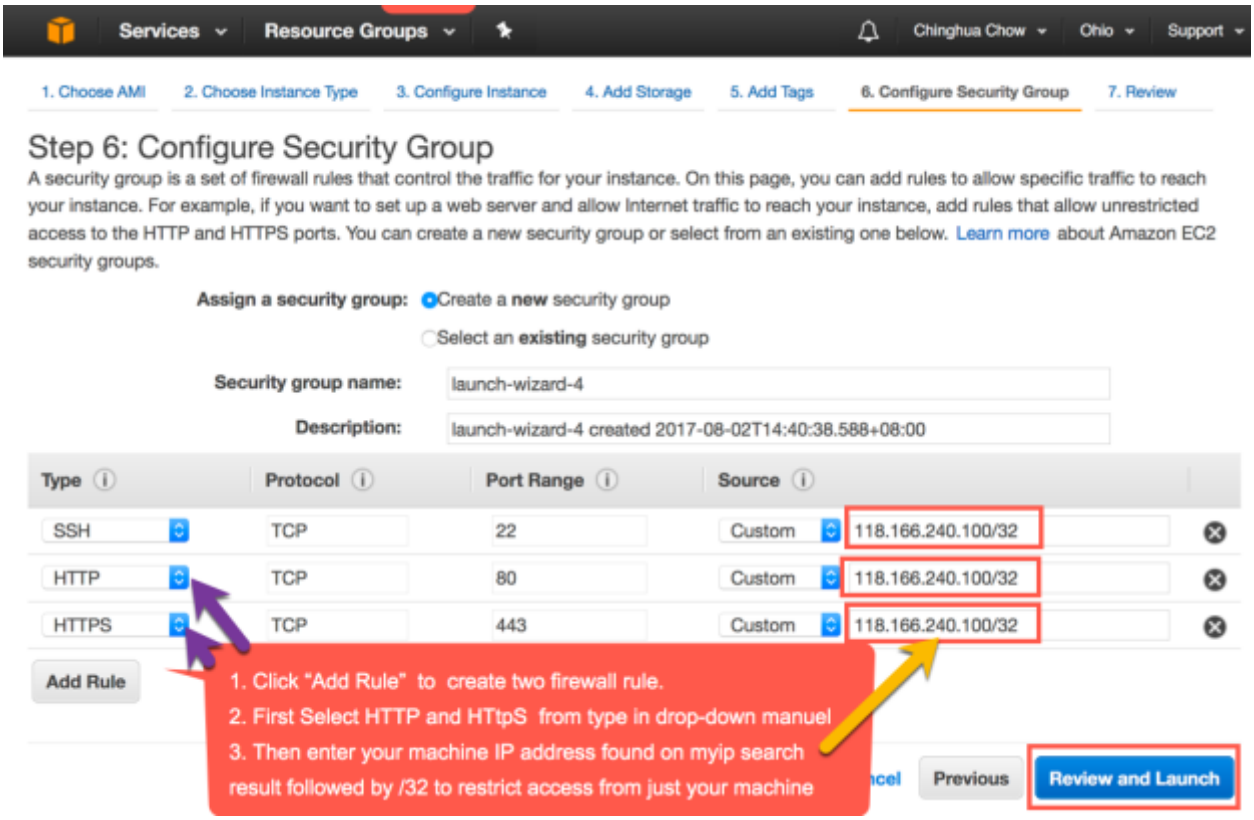


Figure 9. Specify Security Group (firewall) including ports allowed open and source allow in.

Step 7. Review Instance Launch

Click Launch. See Figure 10.

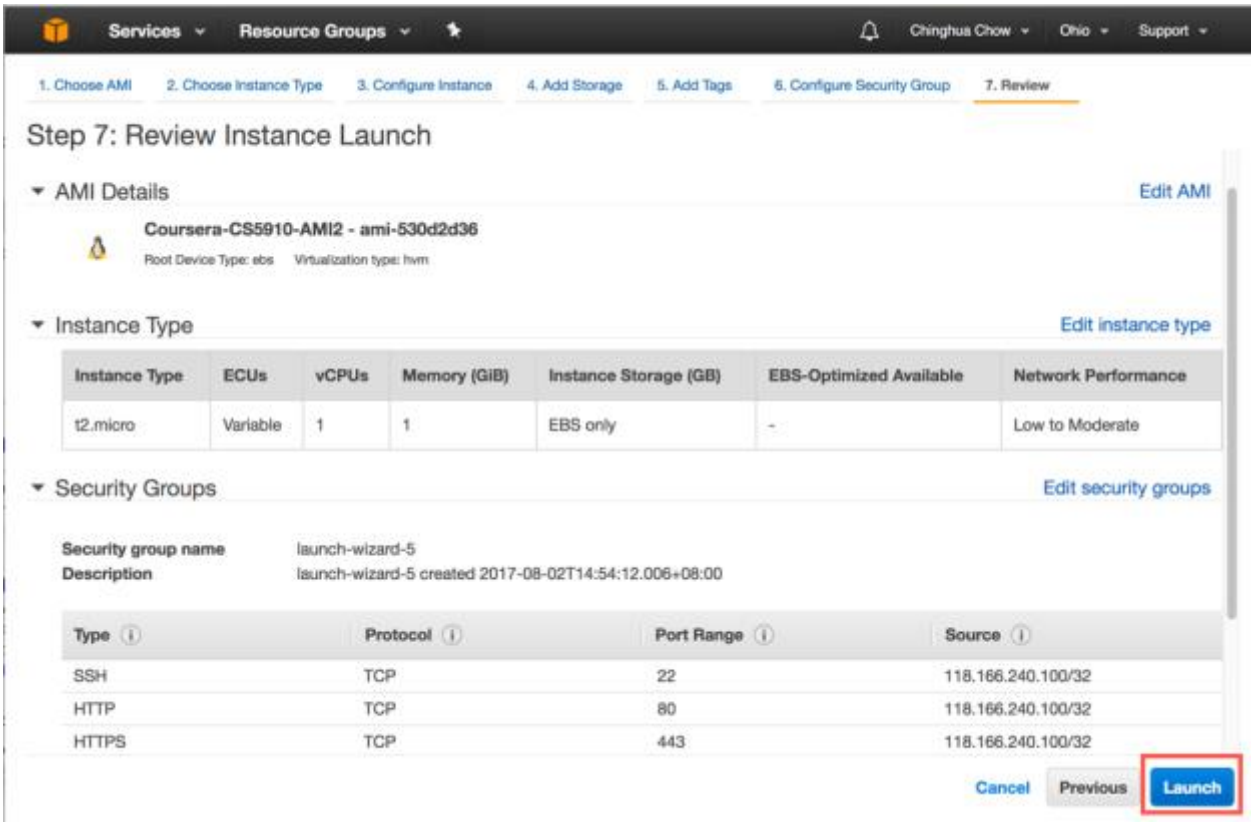


Figure 10. Review Instance detailed chosen for launch.

After click “Launch”, you will prompt to create public/private key pair for accessing the instance. It is a very critical step here! The pop up box shows up. It reminds us to download the private key or use existing keypair. See Figure 11.

Select “Create a new key pair” from the drop down menu; enter private key file name; click “Download Key Pair” Actually here we only download the private key, not public key. The public key is saved in the .ssh/authorized_keys files for verifying of our ssh access later. You must download the private key file now. No more second chance!! Save the downloaded private key to a safe place and duplicated them. Once you lost it, no way to get it back. Click the Launch Instance. Then click the “view instance” button.

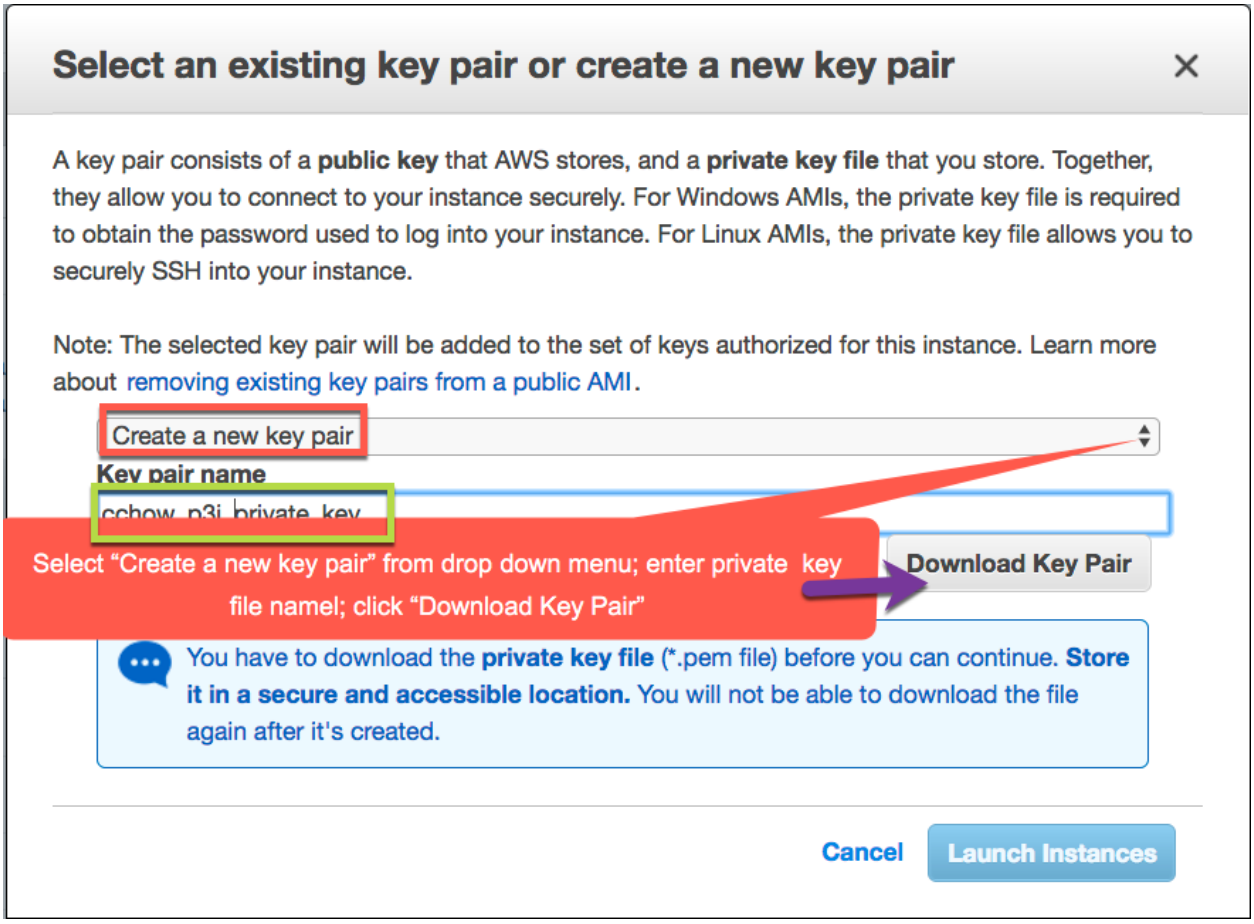
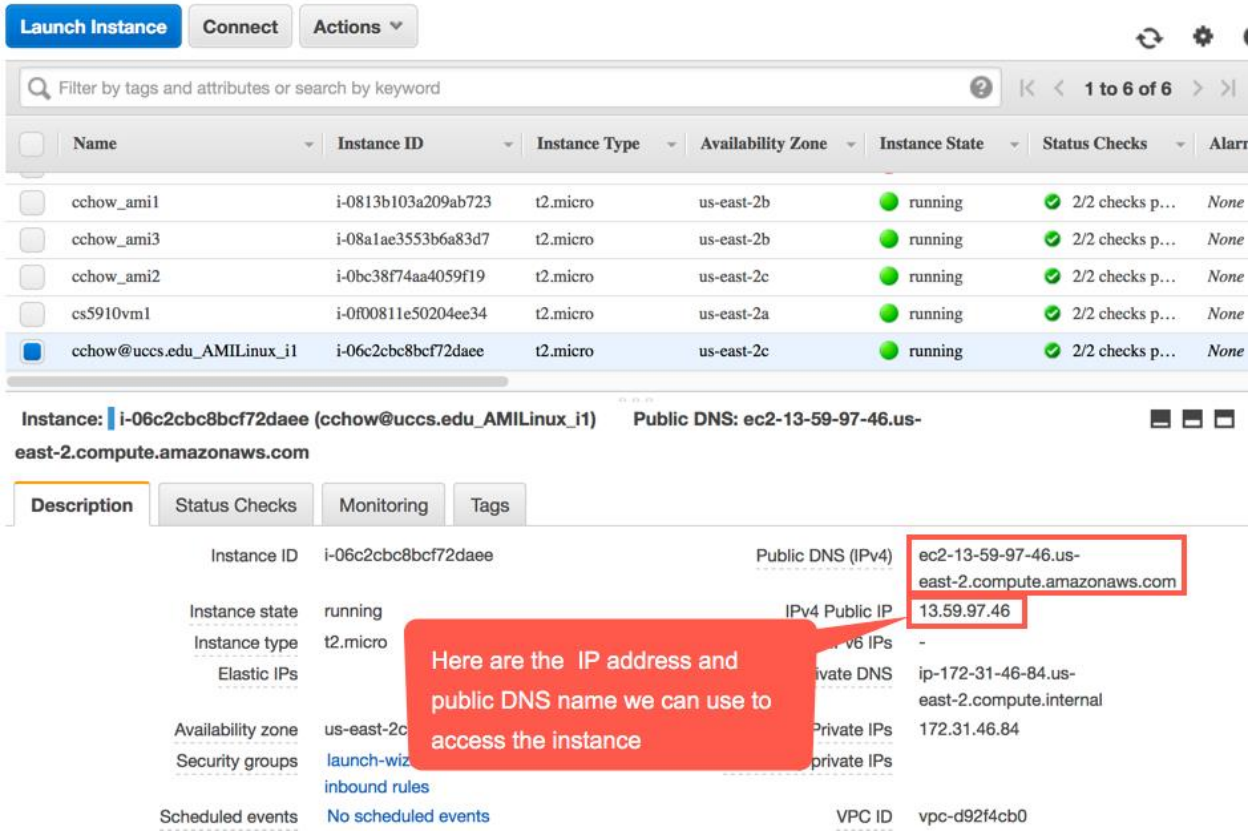


Figure 11. Choose to create new key pair or use existing key pair in the system. Make sure to download the private key (Even though the button say Download Key Pair).

We then went back to the EC2 main interface. Click on the Instances. The instance will be shown to have yellow color and "Initializing", later on when it changed to the green and "Running" as label. Then we know the instance is ready for access and providing services. See Figure 12. Here we see the entry with cchow@uccs.edu_AMILinux_1 as Name of the instance, and next is the instance ID which can be used as a parameter in ec2 api call to access and manage this instance. We will demonstrate that in later session.

When the instance is selected, the lower panel wil show the related instance information. The right side of the lower panel shows the public IP address and public DNS name AWS create automatically for us. It is quite a long name. We see the public IP address is included as portion of the DNS name with -. Later we can show how to create our own shorter domain name if you obtain a dns domain through the Route 53 service. For now ,we can use the public IP address,

which is shorter, to access the instance.



This complete the cloning of an instance. In our specialization, we will ask you to clone the above Coursera-CS591-AMI2 AMI image. Later we will clone a Kali AMI image and a Windows XP image for penetration testing exercise. We can also use these instances for setting up DMZ subnet for cyber defense exercises.