CMIT 495 Current Trends and Projects in Computer Networks and Security
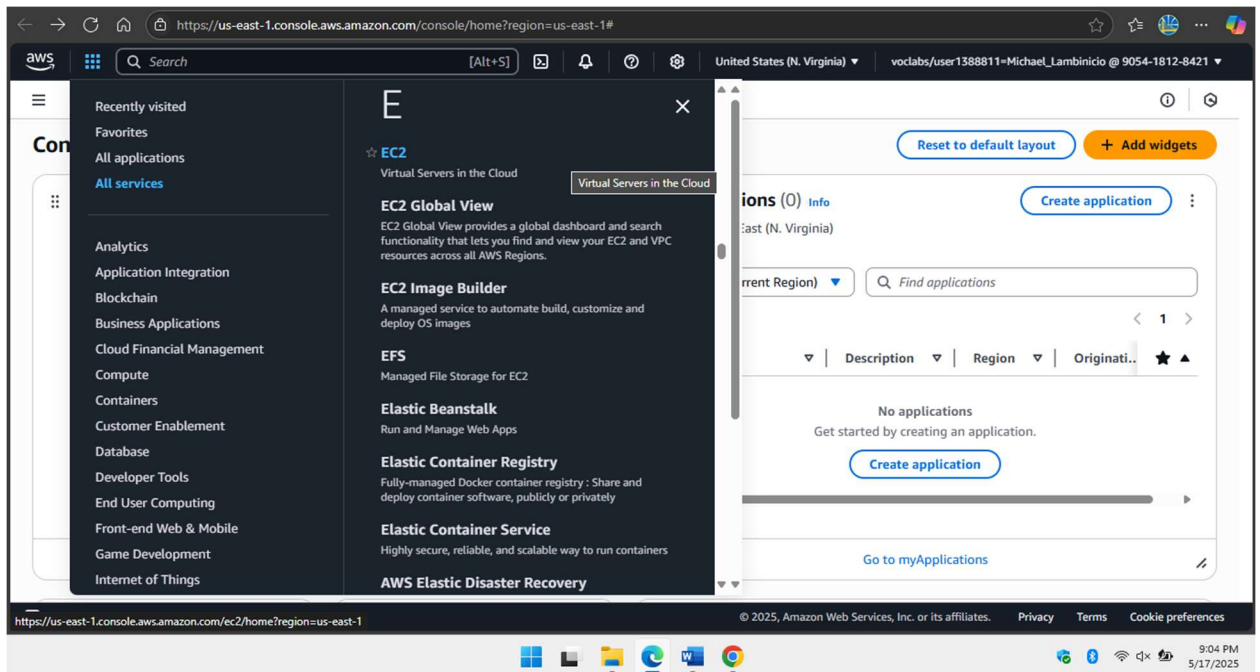
Week 1 – Virtualization

1. Start your AWS Learner Lab (link can be found in the AWS Academy Learner Lab module in LEO). The initial spin-up can take a while, budget five to fifteen minutes for this process. Once the AWS icon on the lefthand side is green, take a screen capture of the AWS Console (Dashboard) and embed it below.
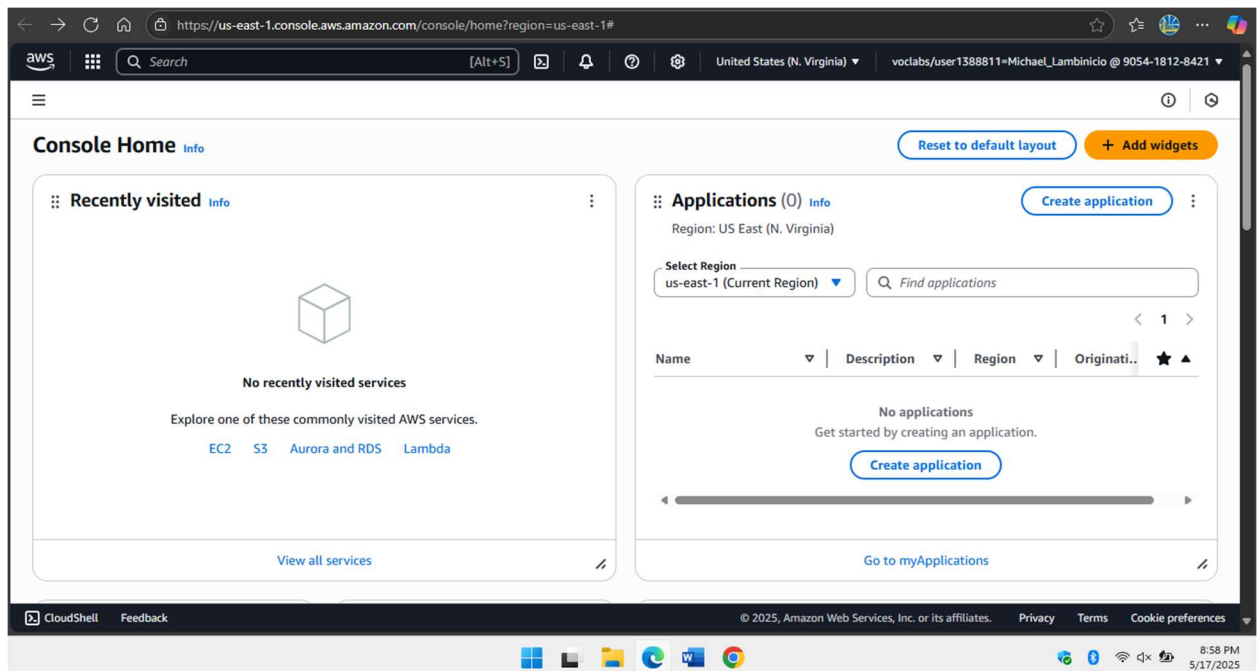

2. Provide a detailed overview of the steps required to provision (create) and launch an AWS Ubuntu-based server virtual instance. The steps may be listed in bullet points or complete sentences. Use as much space as required.

    You will first need to create an instance by using EC2. From the main console, from the services icon (next to the AWS icon), select it and choose all services, select the letter "E" in the alphabet above the next pane over and choose EC2, shown below:
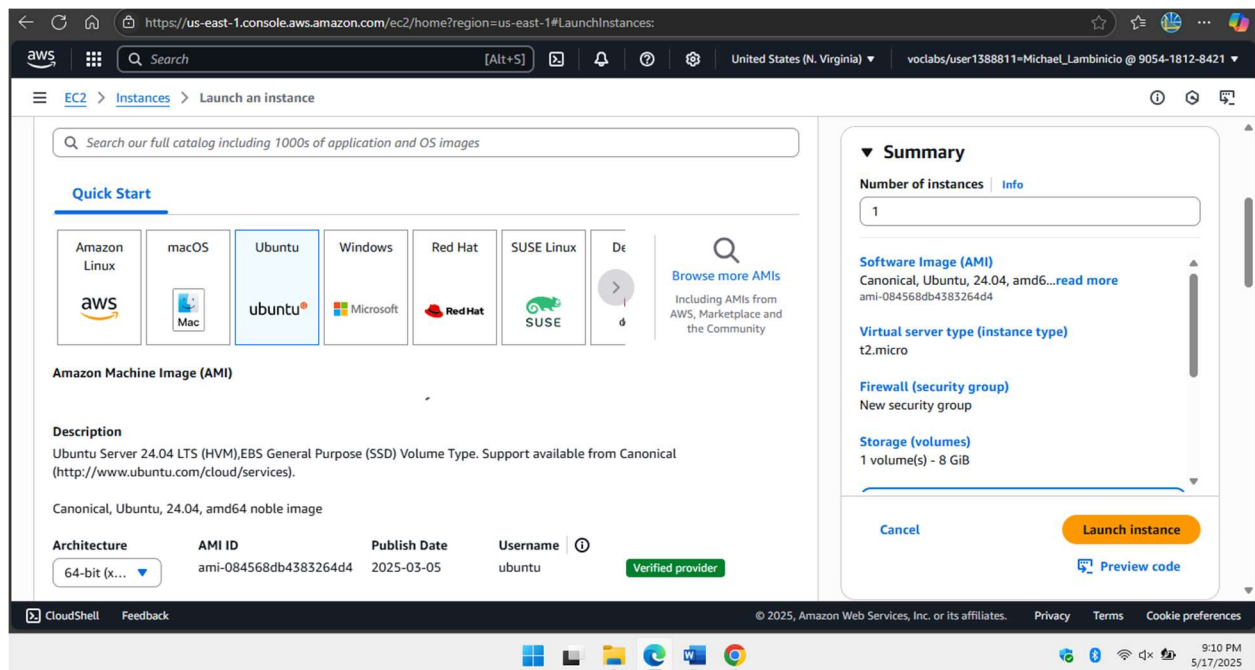
From the EC2 main window, scroll down slightly and choose launch instance that is boxed in orange, shown below:
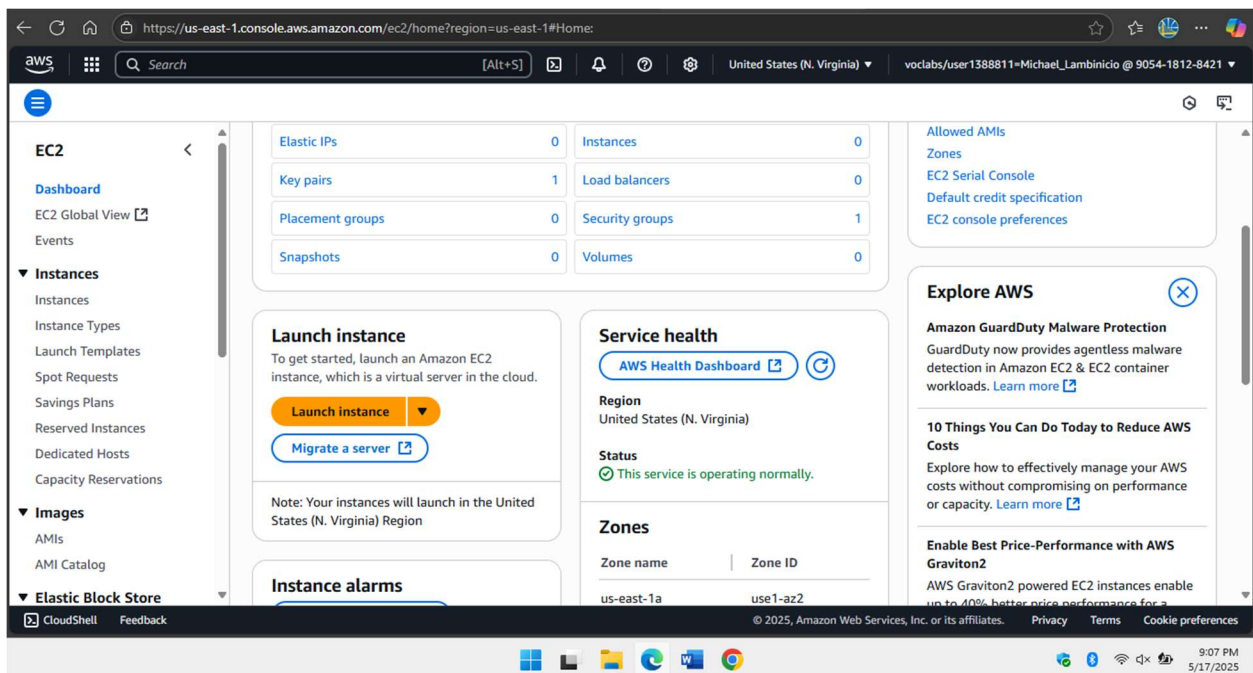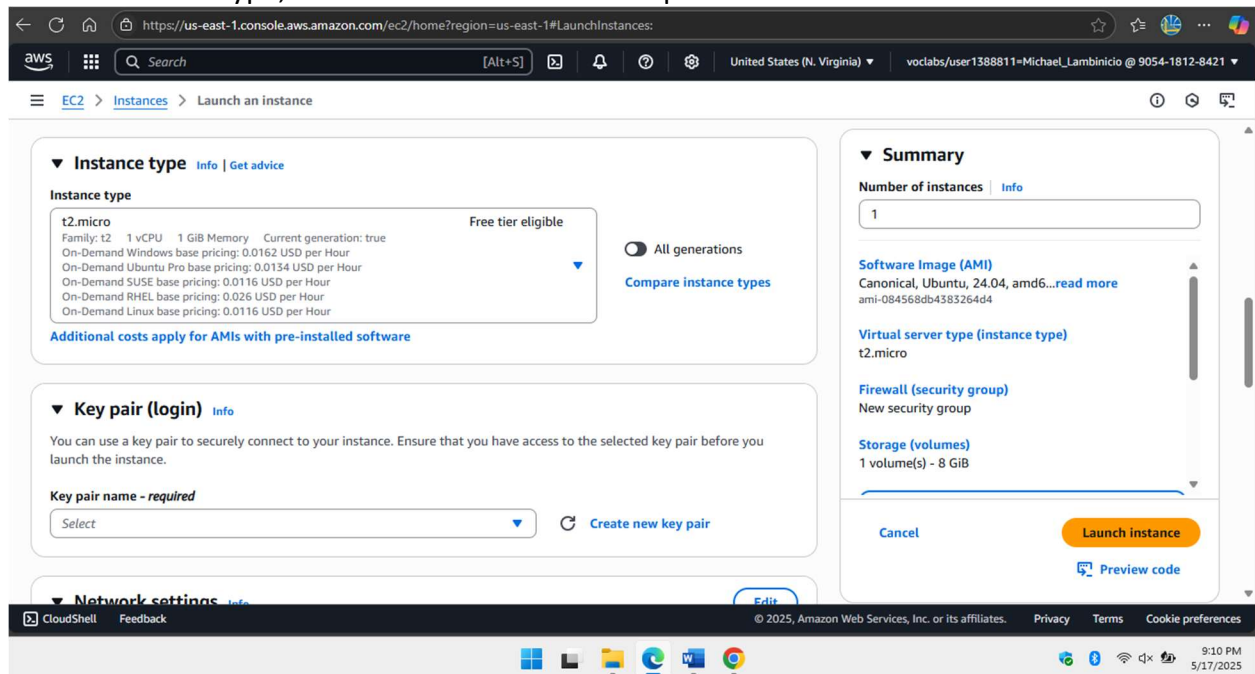

Then, you will type a name for your instance and then choose Ubuntu under the application and OS images.

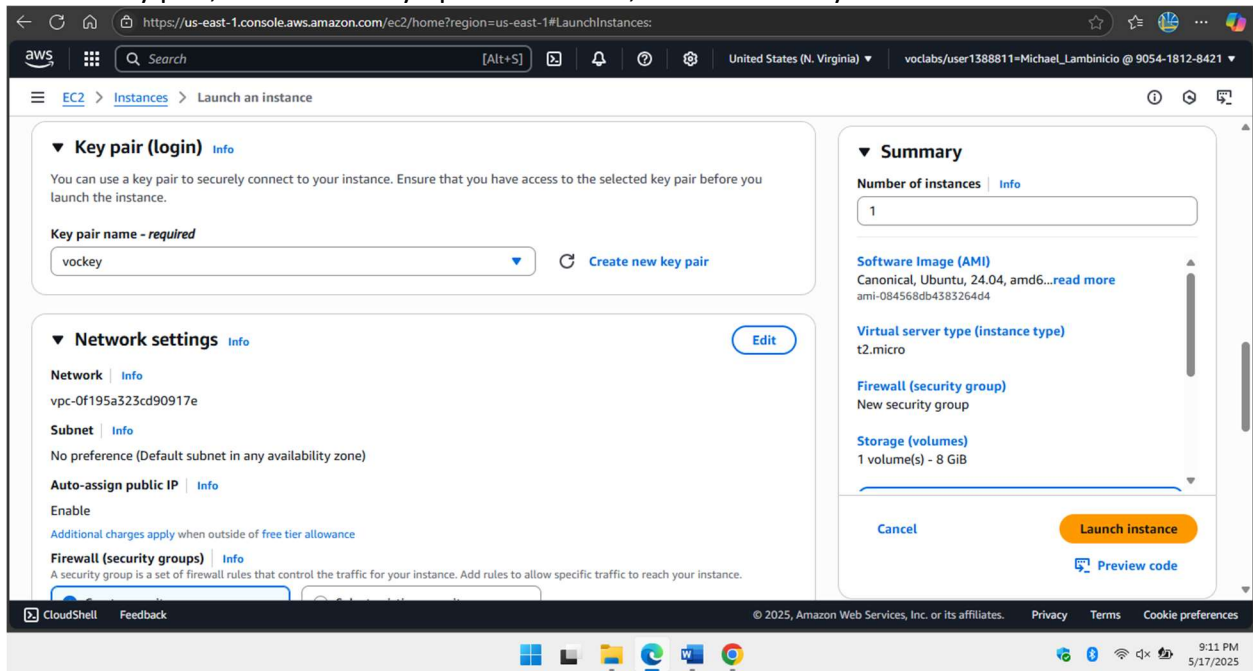*Export/print your completed file as a PDF and upload to your LEO/Assignments folder.*

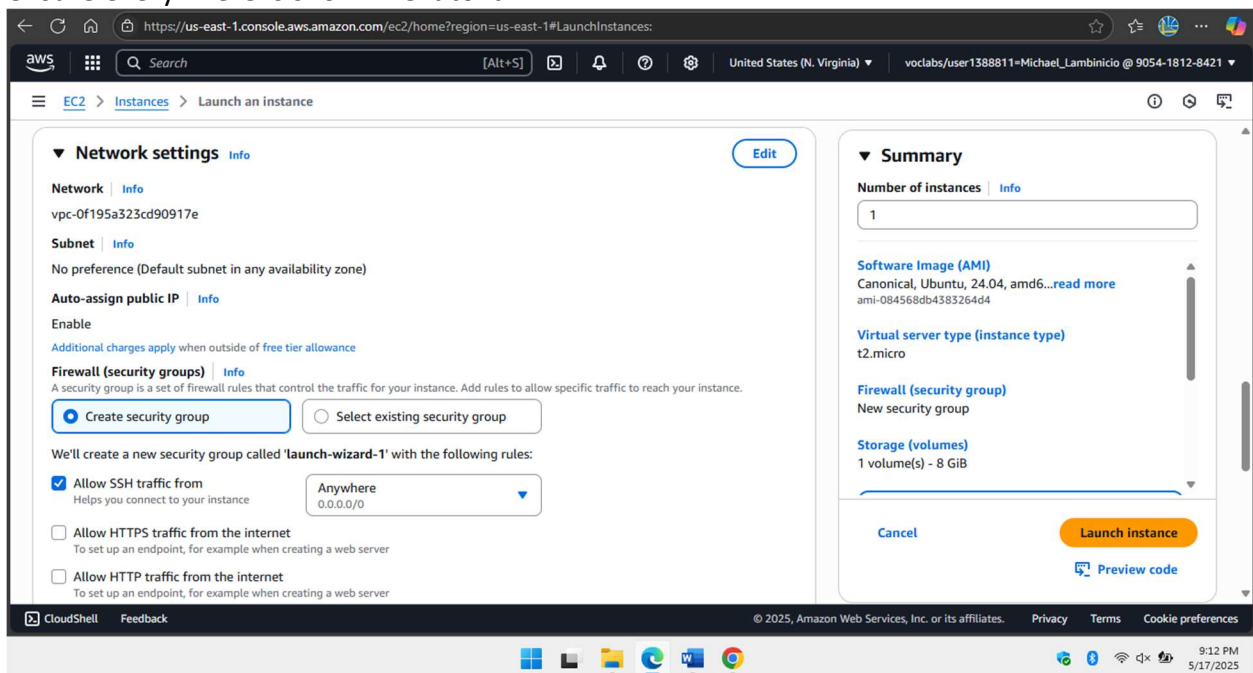On the instance type, choose the free "t2.micro" option.

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

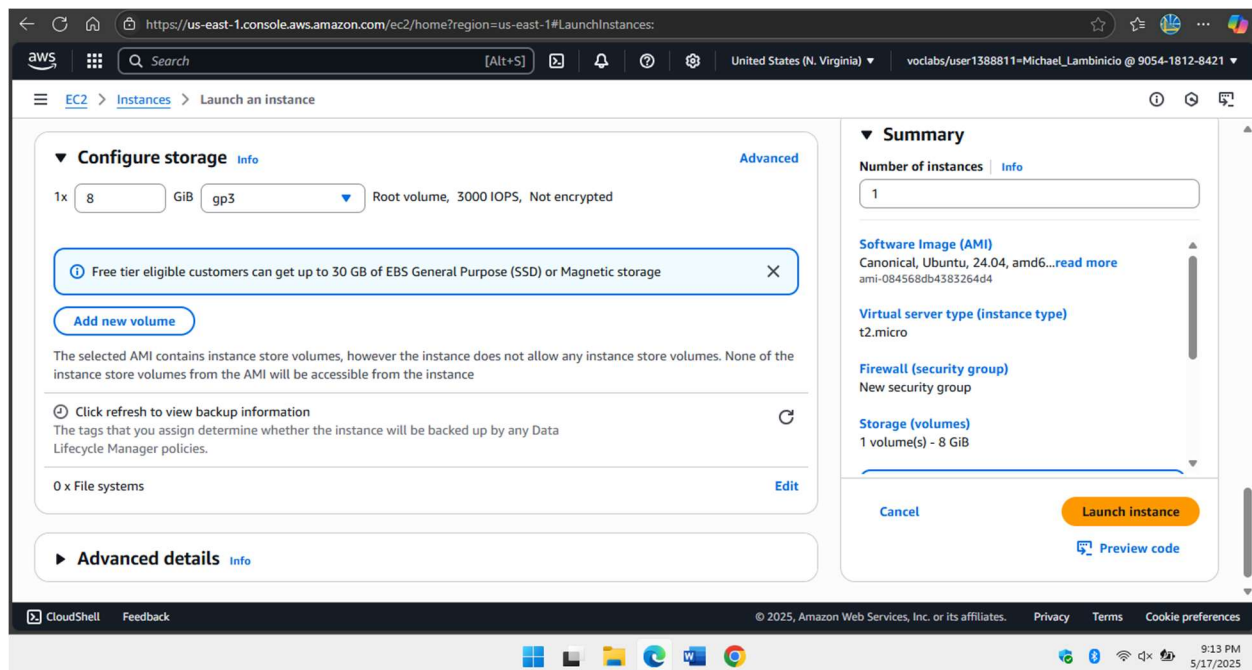For the key pair, select the only option available, which is vockey.

After, the create security group is selected by default, check off allow SSH traffic from and ensure everywhere is shown next to it.
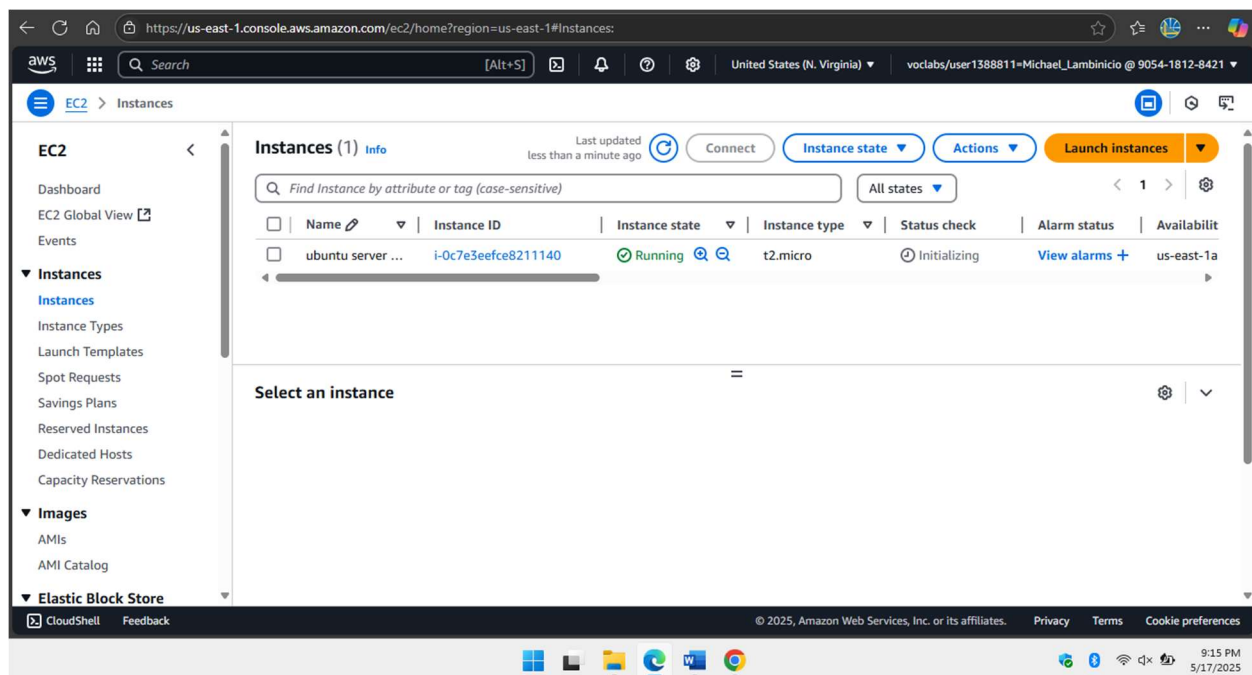

Leave the storage option as is, shown below:

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

After all is set up, click the "launch instances" button highlighted in orange on the right side of the console. It will then show you the created instance with the name you have given.

You may then click on the instance ID to launch the instance to open its console and click the connect button at the top of the console screen to launch it.

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.
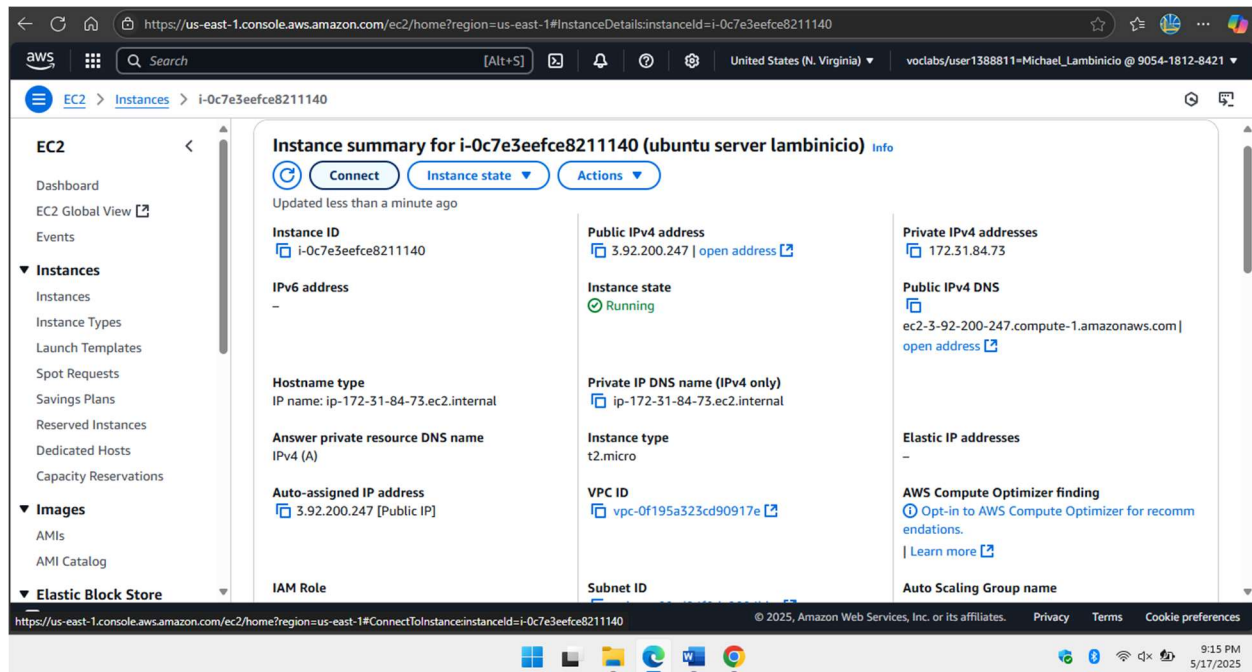
3. What are the benefits of virtualization in a cloud environment? Discuss a minimum of three benefits in detail.

One good benefit of utilizing virtualization is the freedom of owning physical data centers or servers in your building space. You can gain your manpower back in redistributing your personnel who would normally man and maintain those servers to more prioritized assignments to meet deadlines and build stronger infrastructures. You can also use a smaller team to manage the virtualization environment in a central location, rather than separate teams in different areas.

Next, in the event of a disaster, if your physical locations were apart of it, that could cause a financial chokehold since you would have to replace all the hardware lost and then spend more manhours recovering all the data that was lost while informing your customers of the downtime and how long. Virtualization frees you from that as they have specialized teams to tackle these inconveniences while still maintaining minimal downtime.

And the last is cost, speaking of spending more money to replace lost parts in a disaster, just saving in cost in general by moving your environment into the virtual cloud one will allow you to keep the minimal hardware needed and encourage you to gain profit from your hardware to use in possible investments in your future cloud virtualization.

4. Based on your experience, what was the most challenging aspect of provisioning and launching the AWS Ubuntu-based server instance in the AWS virtual environment?

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

The only challenge I had was trying to log in through the local machine using PuTTy. It wouldn't verify my login as name through the downloaded labuser.ppk file because I did not give my instance an IAM role. Once I realized that I had to set the role to the Lab User Profile (pre-set), I was able to then login as a user to provision as needed.

5. Configure your local host computer to use an SSH client application to interact with the newly created and running AWS Ubuntu virtual instance. If using a Windows-based local computer, read over the AWS document, "Connect to your Linux instance from Windows using PuTTY", download and install PuTTY[1] or use Windows 10 built-in OpenSSH client.
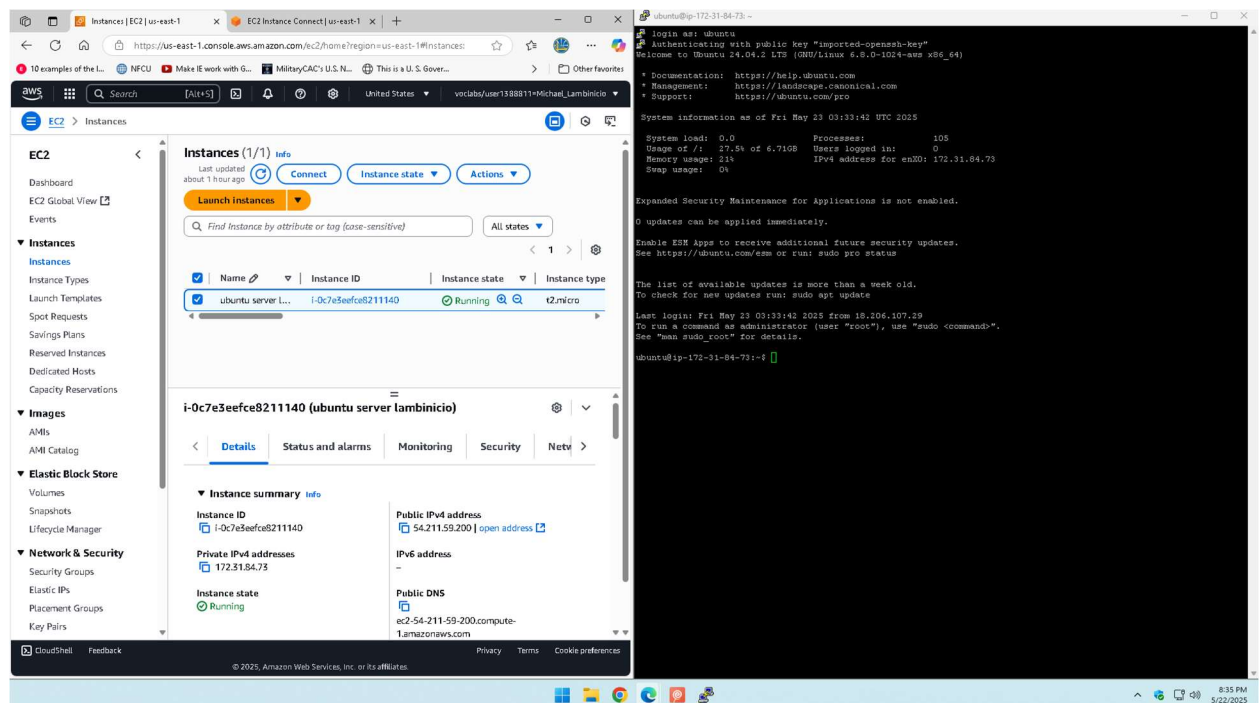
6. From the local computer establish an SSH connection to the AWS Ubuntu Server virtual instance, login, and update the Ubuntu Server using *sudo apt-get update* and *sudo apt-get upgrade*. Perform a screen capture after having each command successfully run.

---

[1] *Link: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html*

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

Sudo apt-get update:

Sudo apt-get upgrade:

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

7. Next, describe in depth what the *update* and *upgrade* commands are doing (explain why it is important to run these commands, how often should these commands be run, where do the commands pull the updates).

It is important to run the update command because it will gather the most up-to-date versions of the software, and all third-party software installed and configured. Upgrading retrieves any updates that have been released from the list you gathered from the doing the update command. There are a variety of frequencies of when to perform these commands, but for the new setup and until the staff are properly trained to function Ubuntu, it is best to utilize the auto-updating package provided by the OS until then.

8. After successfully deploying the Ubuntu Server operating system updates and upgrades, reconnect to the AWS EC2 console, and if needed login again via an SSH client (Note: SSH session inactivity timeout is short). Instructions to SSH are provided by Amazon on how to do so. When connected, run the following commands to obtain information about the host and network settings (perform a screen capture of the results and embed below):

echo '<your name>' && echo 'CMIT 495 <your section> <your semester>' && date (section is a 4-digit number like 6380 and semester is a 4-digit number like 2215 or 2218)
whoami
ip
pwd
ping -c 4 www.google.com

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

9.   What kind of account did you discover when you ran the *whoami* command? How do you know?

When the command was run, it concluded with ubuntu, claiming it as a user account. You can tell the difference if you were to use "sudo" in from the "whoami" command. When that is typed, it will output root. You can tell when you are using a user account by results not showing root, or system accounts.

10.   Note the difference between IP addresses—specifically, when you perform the *ip a show* or *ipconfig* on your personal system, versus the *ip a show* command within the EC2 instance VM command prompt. Describe the network settings of each system. Why are the IP addresses different? Are the IP addresses private or public? What is the difference between a public and private IP address? Explain in detail.

The EC2 VM is an added layer on top of a system that already has an OS set up. This means that when the instance is set up and launched, it creates its own virtual NIC (or network interface adapter) which would need access to the physical external network. Then, it would use NAT (or network address translation) to share the network if needed. Most virtual machines are set up privately so they would have private IP addresses.

11.   Virtualization allows us to place the functionality of many servers into a single host while maintaining configurable levels of separation between all virtual machines. How do you believe virtualization could help in data center consolidation? What would you be leery about during and after any transition?

It is such a big benefit of consolidation when using virtualization. Each virtual server can be layered differently to accommodate certain standards staff teams that are created to use without having to re-do each one. This would allow each user who needs the resources to do a certain job to have them readily available with a VM that has already been preloaded to get them started. This would also allow the datacenter to have flexibility, scalability and manageable standards to prevent any failures.

Something to be leery about would be the fact that because you are using a provider for virtualization, if a disaster recovery plan isn't described to you during your agreement, any failure with no redundancy will cause a major problem for your organization and may cost a lot of money to rebuild all lost assets.

12.   Does virtualization increase the cybersecurity posture of the organization? If so, describe how and why. If not, describe how and why not.

It would absolutely increase the posture as a big benefit to the organization. Cloud services who offer virtualization have dedicated teams almost 24/7 to monitor any unusual activity that would affect your organization. To add, you will also have virtually no physical hardware in locations that would not be monitored at any moment that can

Export/print your completed file as a PDF and upload to your LEO/Assignments folder.

cause an attacker to steal it if they are unable to penetrate. You are also given the ability to capture an attack instance and isolate as needed to evaluate, eliminate and prevent it from happening again.

13.   There are various virtualization options: bare-metal (Type 1) in which the hypervisors run directly on the hardware as their own operating systems, and user-space (Type 2) hypervisors that run within the conventional operating systems. Which of these options is more secure? Describe the vulnerabilities you believe exist in either Type 1, Type 2, or both configurations. What do you believe can be done to mitigate these vulnerabilities?

Type 1 hypervisors are believed to be more secure than Type 2. Because Type 2 is "layered" on top of an operating system, vulnerabilities can happen at the operating system stage which can ultimately affect the hypervisor. It would make it even worse if you had multiple hypervisors on one operating system and if an attack happened on that one operating system, essentially your whole operation would fail. Type 2 hypervisors would need a lot of attention to ensure this doesn't happen and you would also have to plan for not having too many on one operating system, or have some type of redundancy and disaster recovery plan.

14.   Confirm that you have <u>stopped</u> and <u>terminated</u> your AWS Linux server instance. To confirm, simply type your name below.

Michael Lambinicio