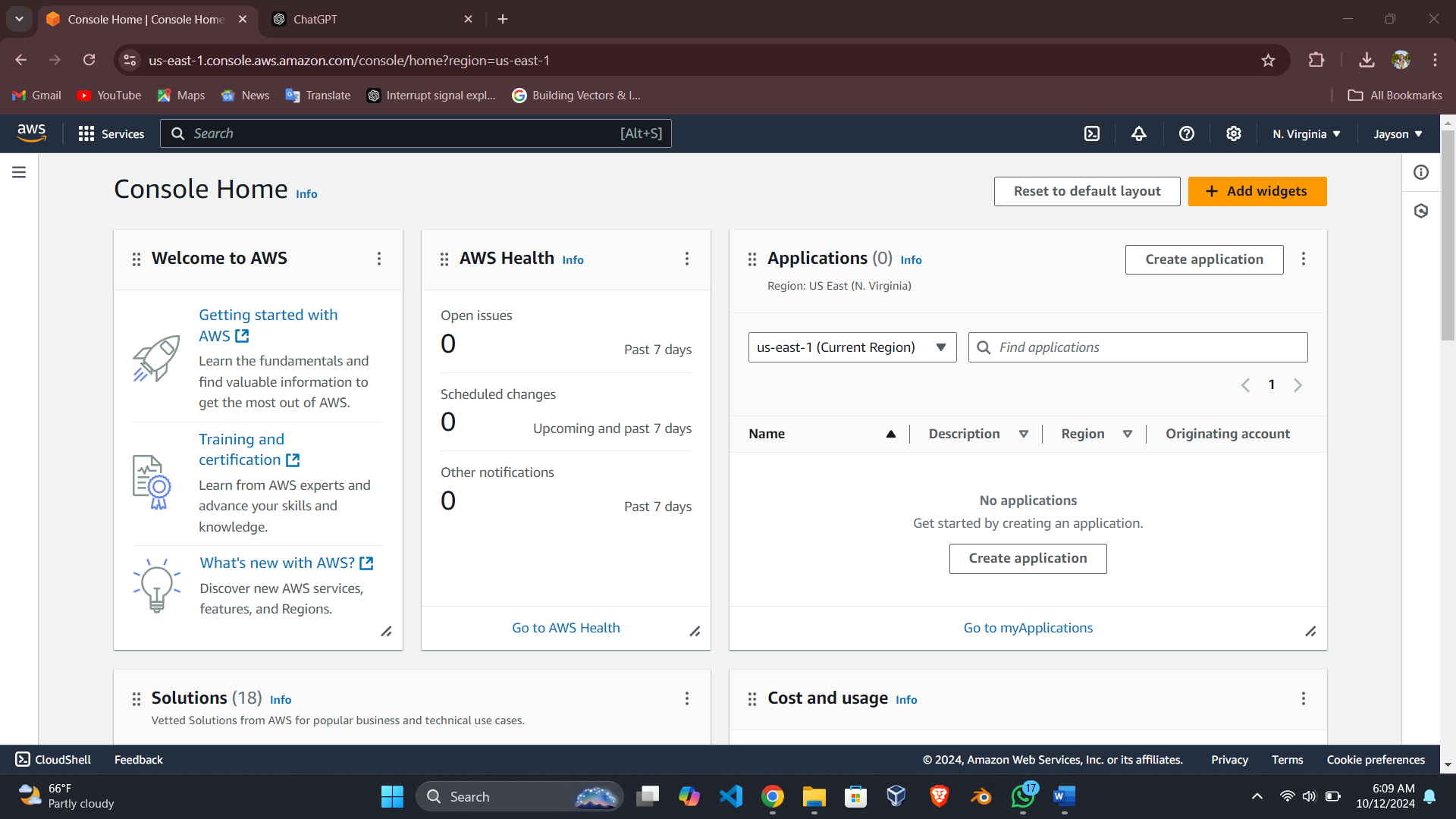
**CMIT 495 Current Trends and Projects in Computer Networks and Security**

*Week 1 – Virtualization*

1. **Log in to your newly created AWS account and take a screen capture of the AWS Console (Dashboard) and embed it below.**



Screenshot 1: My AWS console dashboard.

1. **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.**

1. Log into AWS Console.

2. Navigate to the EC2 Dashboard under Services and click on instances.

3. Click Launch Instances.

4. Enter the name of the instance you want to create.

5. Choose ubuntu as the Application and OS Images

6. select Amazon Linux 2023 AMI(free tier) under Amazon Machine Image

7. On instance type choose t2. micro which is eligible for free tier.

8.Choose create a new key pair, the authorization credentials will be downloaded

automatically.

9. Enter your desired key pair name

10. Under private key file format select PPK for use with PuTTy

11. Then click in create key pair

12. Under Network Settings select create new security group and select allow SSH traffic

Private key file format

13.Optionally you can allow HTTP or HTTPS if you plan on hosting a web service.

14. You can add storage or leave defaults.

15.Review and launch the instance.

1. **What are the benefits of virtualization in a cloud environment? Discuss a minimum of three benefits in detail.**

1. While resource efficiency can be also defined as a potential for effective use of resources within a concern, cost savings are considered as the major component of resource efficiency.

Through this technique, cloud providers can make optimum use of physical resources by housing multiple virtual machine on a single, physical host. This optimizes resource usage because:

-Less hardware is required: The fact is that by using virtualization, organizations can run the number of instances on the significantly fewer physical servers necessary, thus avoiding the need to buy and maintain quite a lot of hardware.

- Lower operational costs: It decreases power consumption, cooling needs and physical space, which translates into substantial expenditures for very large data centers.

- Pay-as-you-go model: Some cloud providers use the draw business model where companies are only charged the amount of compute, storage and network that they have used.

By extending structure resources to the cloud, no capital-intensive investments are required and companies are in a position to use a flexible Operational Expense model.

2. Scalability and Flexibility

One of the primary benefits of cloud virtualization is its ability to scale up or down dynamically:

• On-demand resource allocation: Cloud resources which have been virtualized can be resized dynamically to meet various needs. For instance, a company during a busy period can quickly add more virtual machines to meet the traffic demand, or can remove them during a low traffic time.

• Global accessibility: In cloud technology, virtualization allows customization of resource accessibility hence making it easily available across the whole world via the internet. This way there will be a guarantee that some services are available at any time and place.

• Multi-tenancy: It is the ability to allocate several users or applications on one physical network and at the same time their data and resources are protected from interference with one another.

Another advantage of cloud environments as consumer enable users to quickly deploy new habitats, such as testing, development, production, and so on are easier to be more flexible to try and introduce new changes.

3. Disaster Recovery and HADR

Virtualization in the cloud enhances an organization's ability to recover quickly from hardware failures or disasters:

• Snapshots and backups: Information technology environments that are virtualized can allow a virtual machine to be copied at a specific point in time and if there should be a failure of any particular system then it can always be backed up easily. This keeps system outages low and enables faster get-well times of important applications.

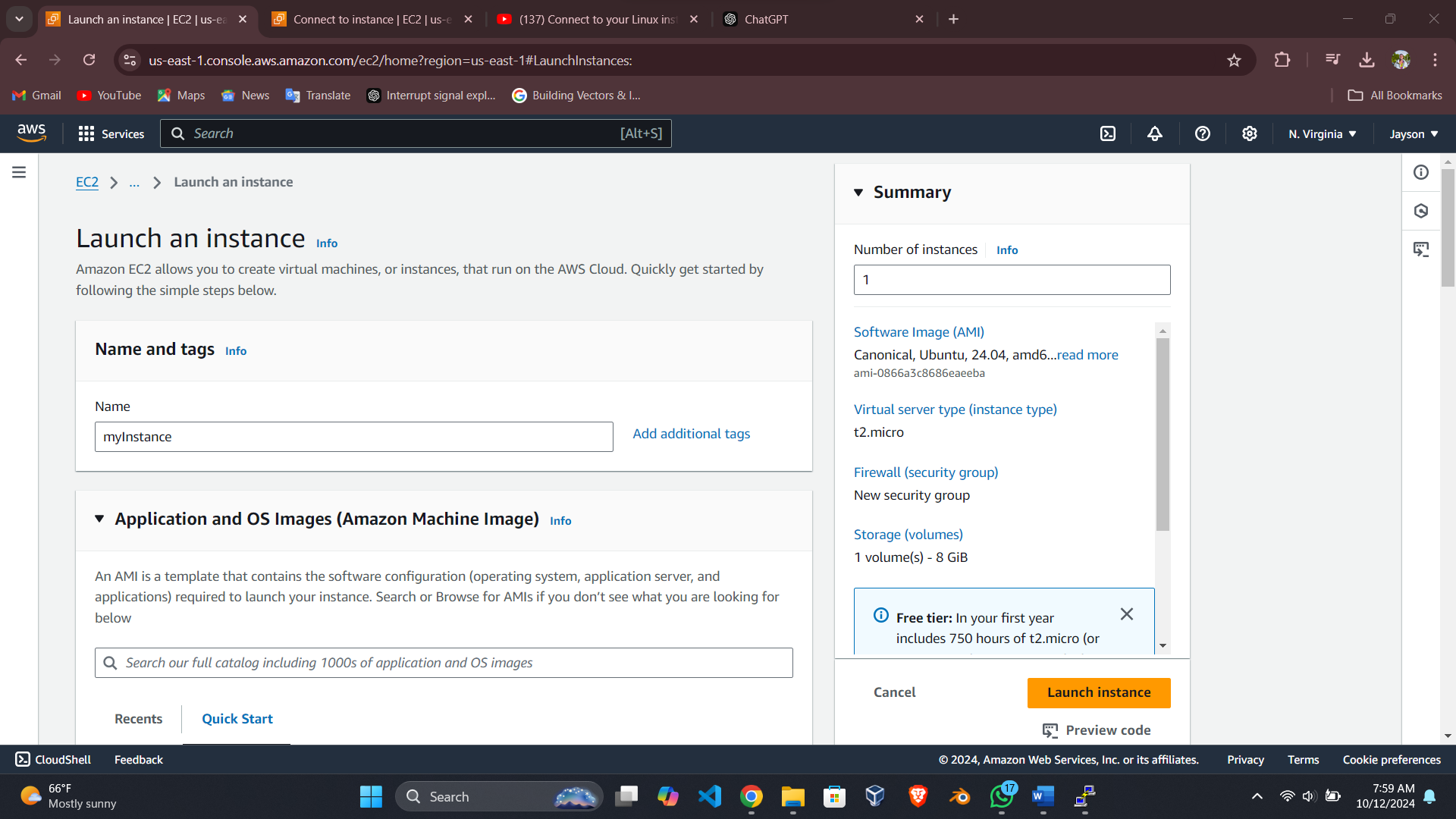
• Redundancy and fault tolerance: As a rule, virtualized infrastructure implies its high availability. a physical server can experience a problem that could be disastrous if not well solved whereas numerous virtual machines can be relocated to another well functional physical server without necessarily affecting services.

• Geographic redundancy: Most cloud providers will copy your instances and data to various locations geographically so that if a datacenter is catastrophically damaged, your systems can continue seamlessly, in another datacenter.

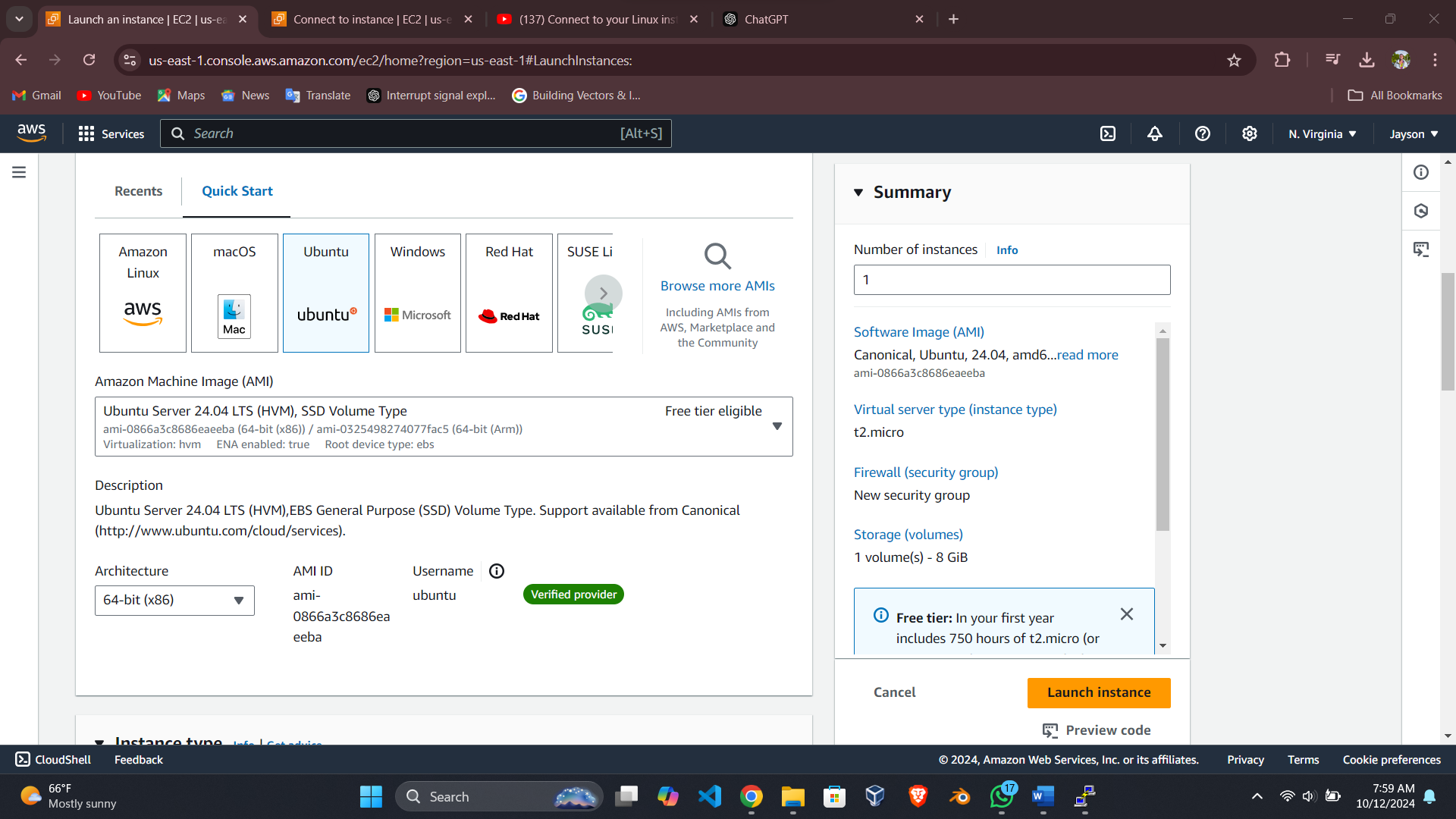
1. **Based on your experience, what was the most challenging aspect of provisioning and launching the AWS Ubuntu-based server instance in the AWS virtual environment?**

The difficult and challenging part of deploying the AWS Ubuntu server was to properly set up the right Security Group to allow the right traffic in and out while still being extremely secure at the same time. To make sure that only required ports should be opened for outside access one has to be very much concern.

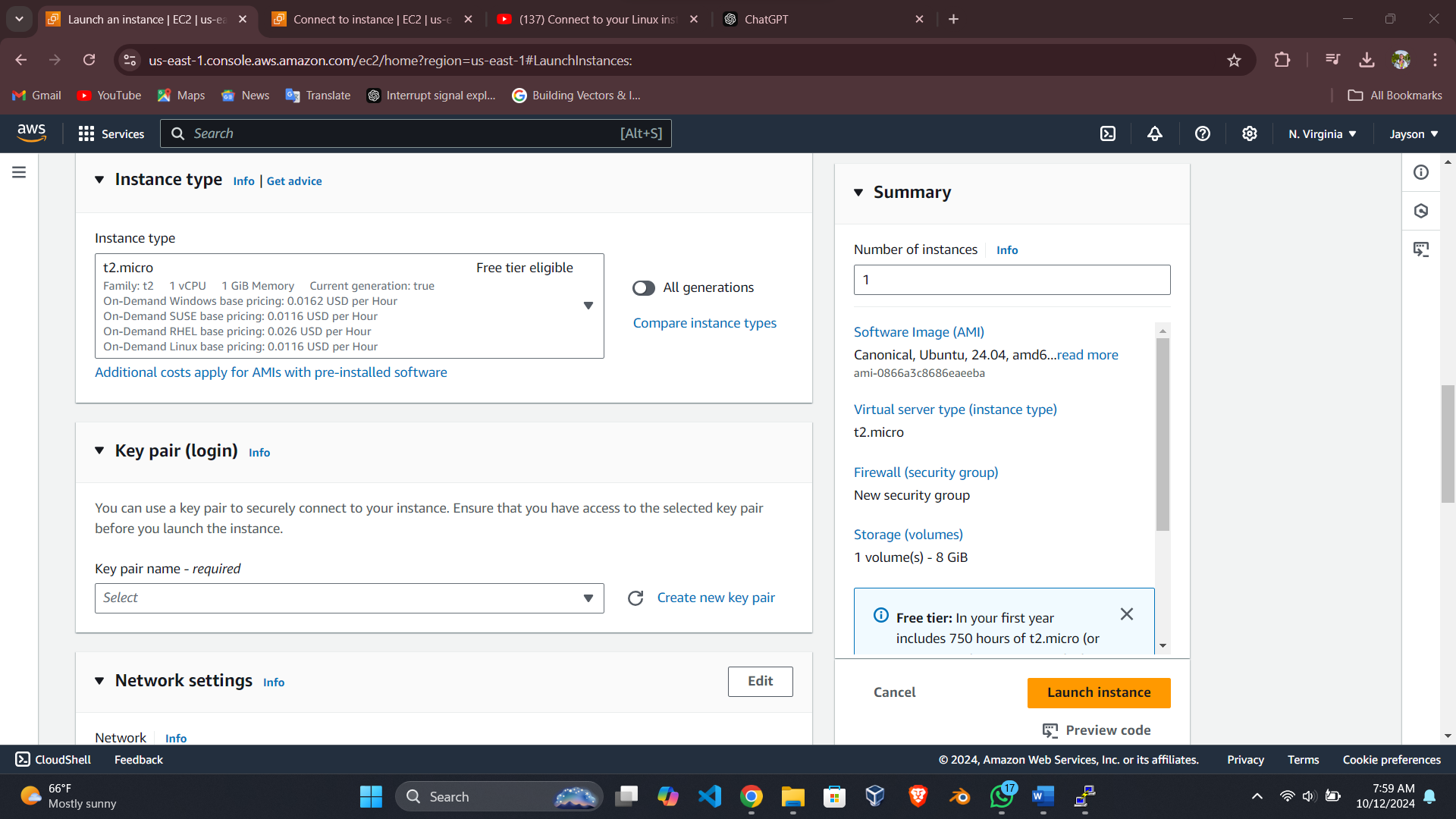
1. **Configure your local host computer to use an SSH client application to interact with the newly created and running AWS Ubuntu virtual instance. If using a Windows-based local computer, read over the AWS document, "Connect to your Linux instance from Windows using PuTTY”, download and install PuTTY[[1]](#footnote-1) or use Windows 10 built-in OpenSSH client.**



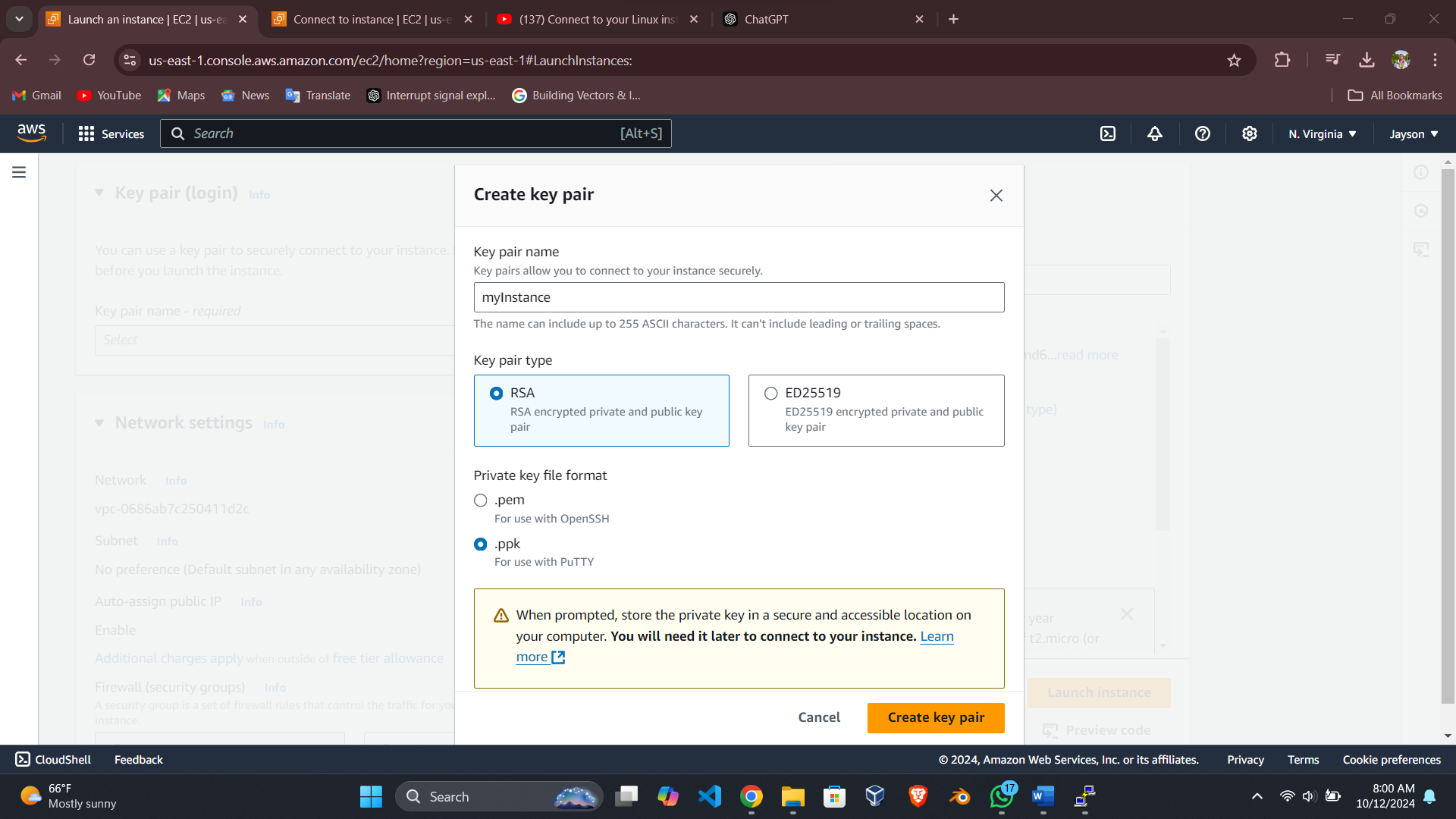
Screenshot 2: EC2 dashboard.



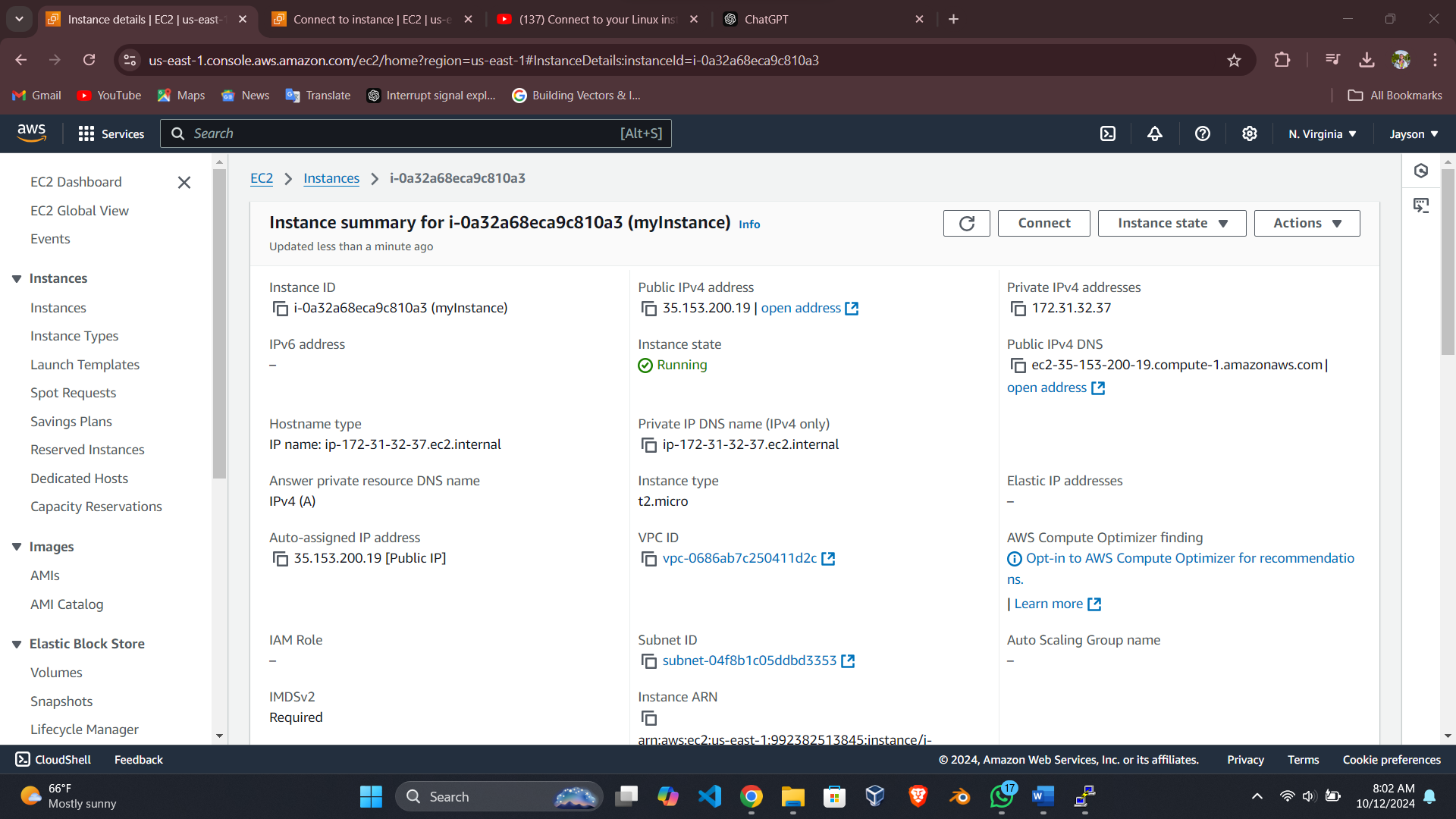
Screenshot 3: Choosing the OS and Virtual Image



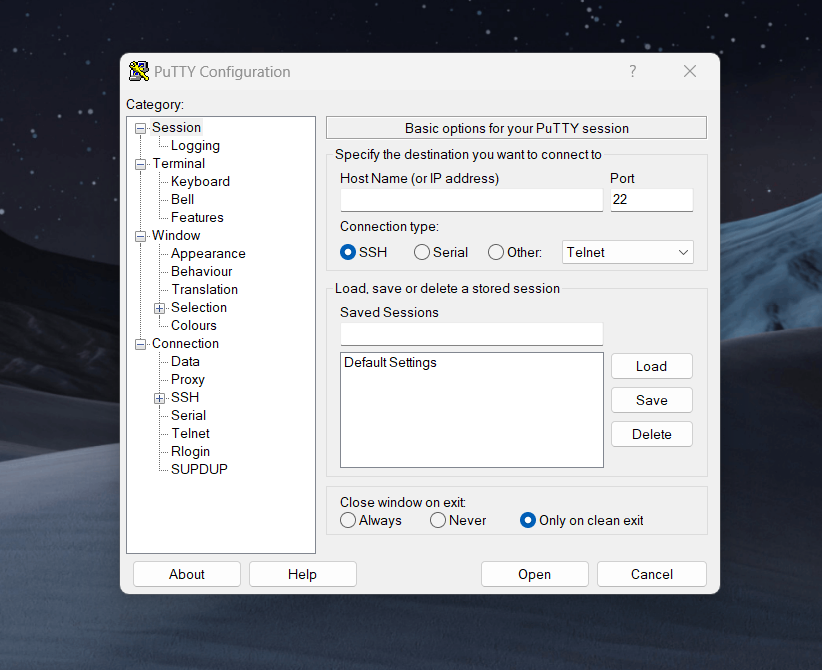
Screenshot 4: Selecting the instance type.



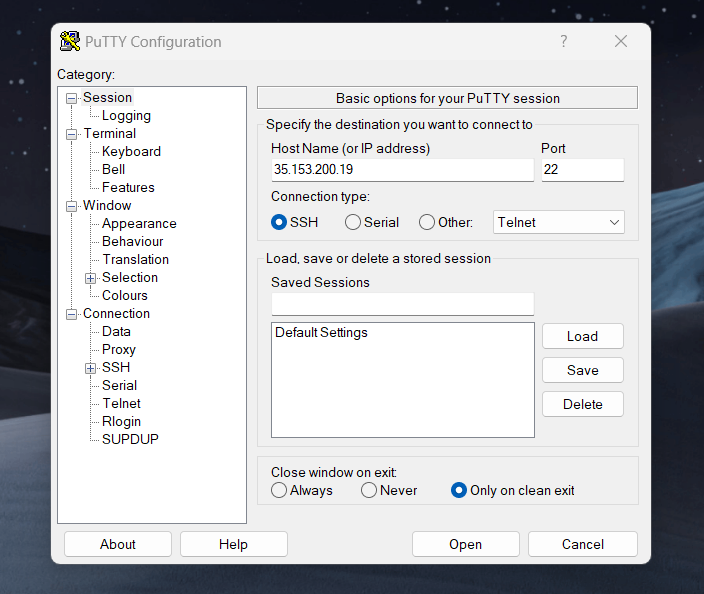
Screenshot 5: Configuring the Key Pair



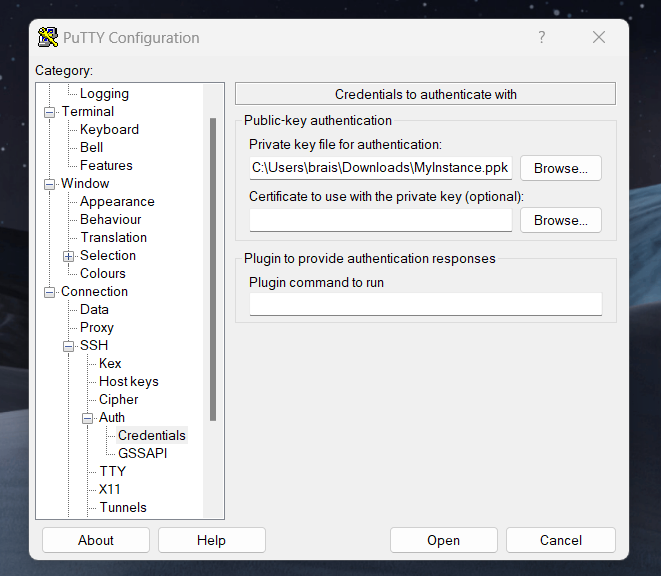
Screenshot 6: Summery of the instance I created



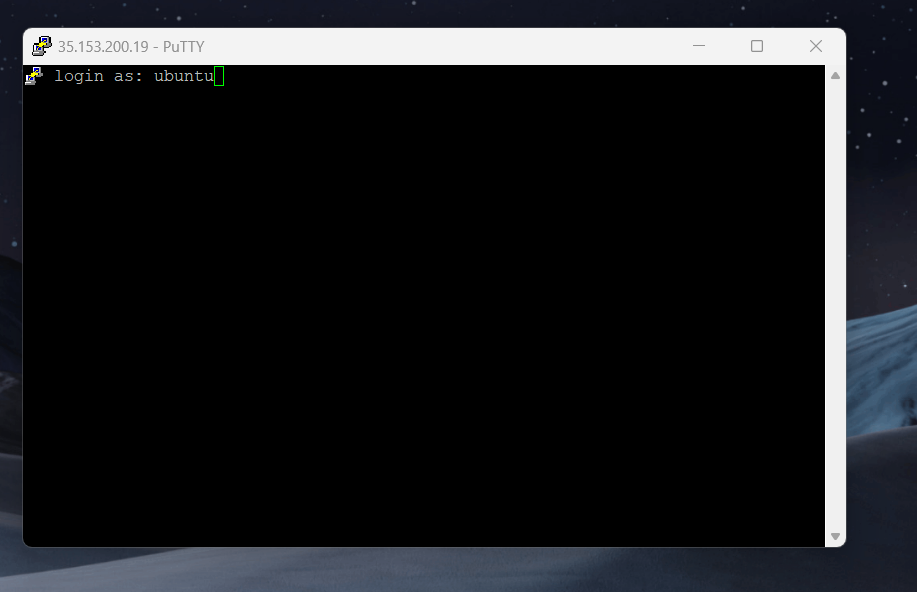
Screenshot 7: Launching PuTTy.



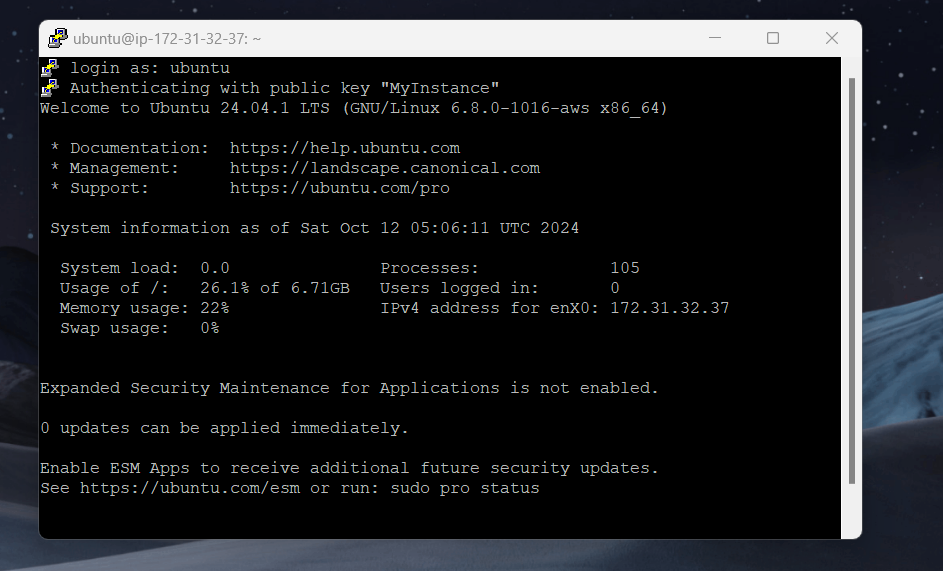
Screenshot 8: Configuring the public ip address



Screenshot 9: Adding the credentials file.

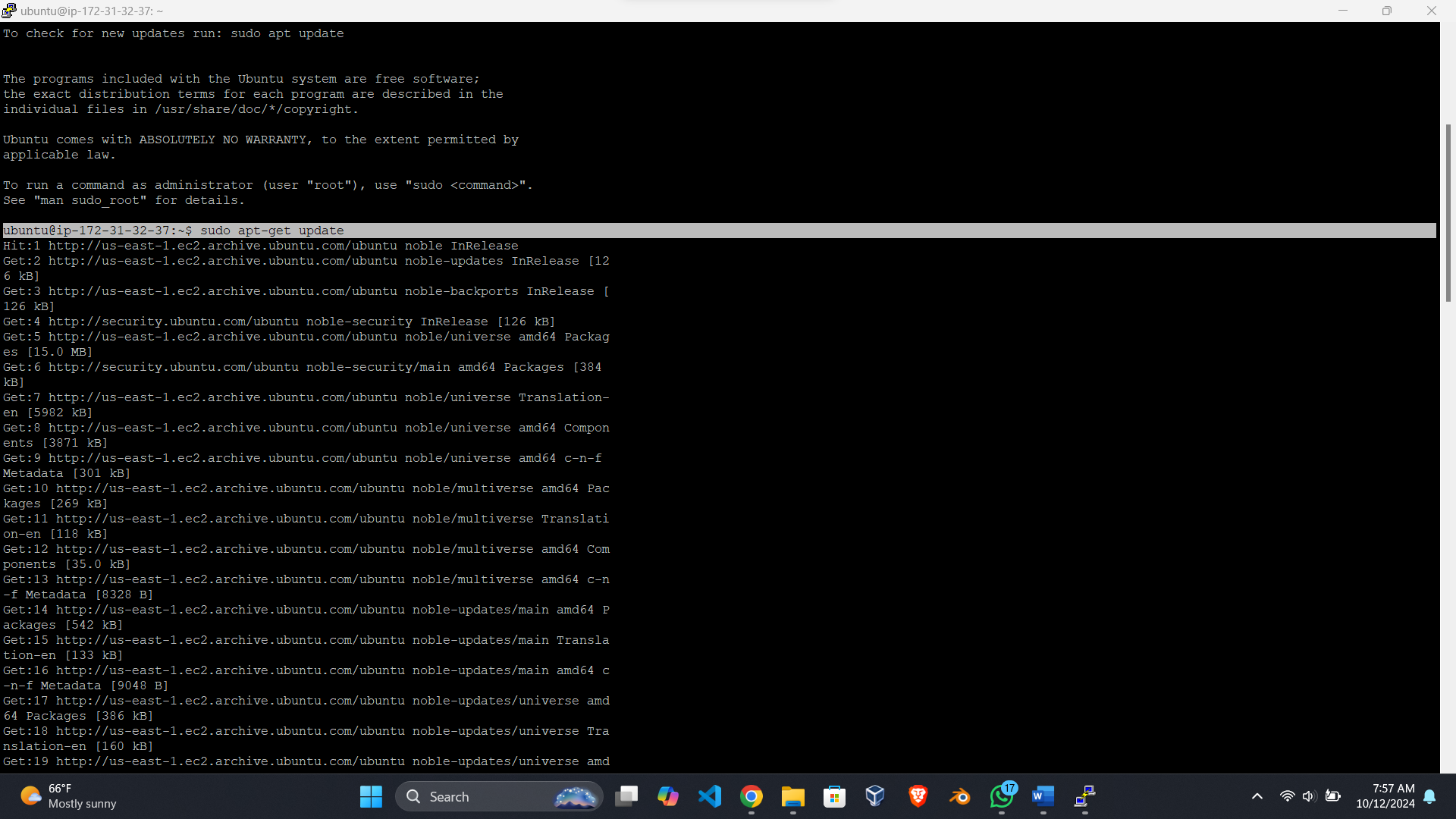


Screenshot 10: Providing the username for authentication.

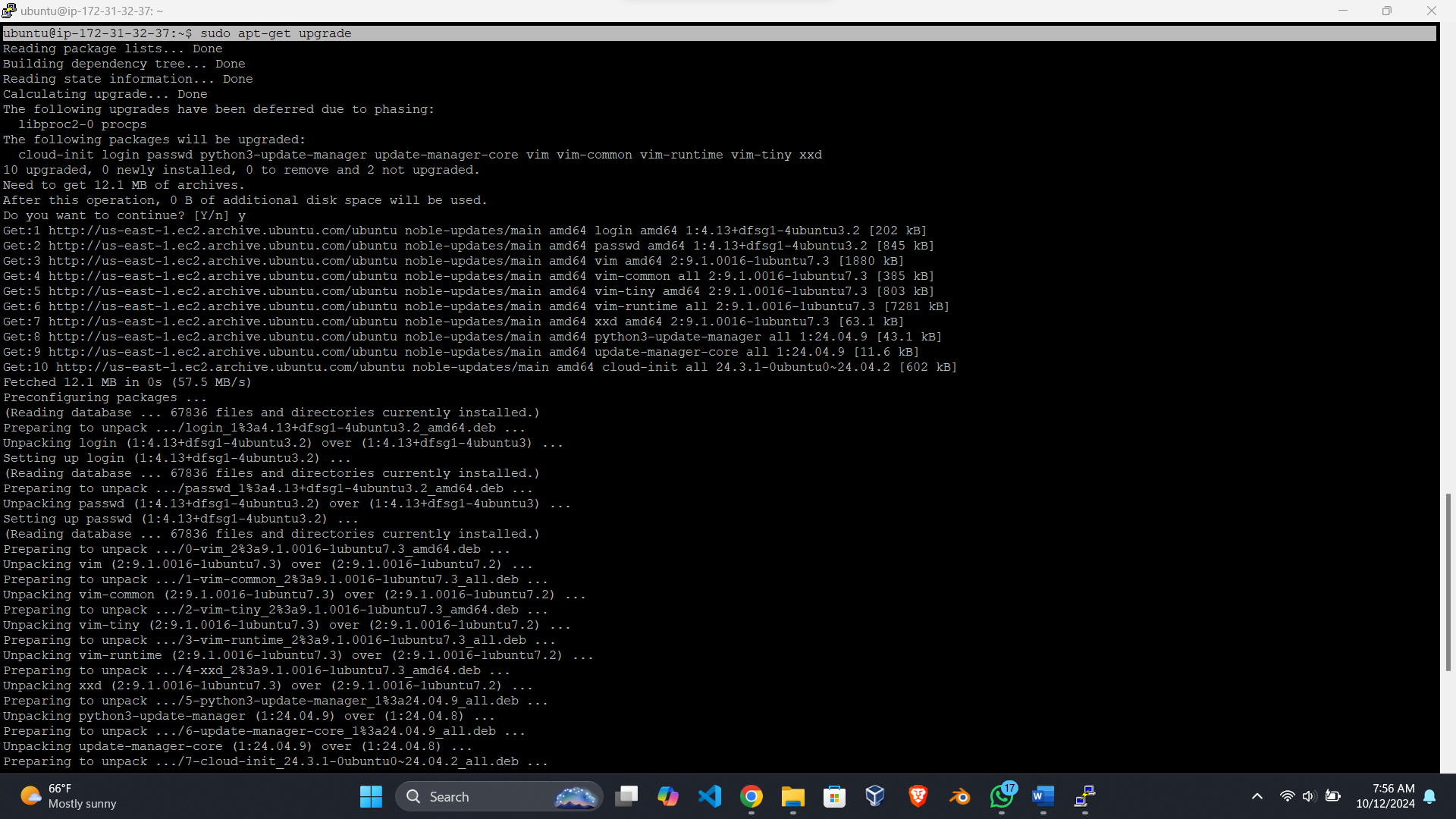


Screenshot 11: Successful authentication

1. **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.**



Screenshot 12: running the "sudo apt-get update" command.



Screenshot 13: Running the "sudo apt-get upgrade" command.

1. **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).**

1. sudo apt-get update

The update command is used to retrieve the latest package list contain the version of the software packages and dependencies available from repositories (software sources).

What the Command Does:

Fetches package lists: Lists of new software packages are retrieved from the sources which are listed in the files /etc/apt/sources.list or in /etc/apt/sources.list.d/.

Does not install updates: This command does not download anything on your system, it does not install software or update them; it only gets you information on the available software, their versions and their dependencies.

Checks for new versions: They notify the system of versions of installed software, making the system alert of the new packages that can install.

Importance of Running update:

Keeps your system in sync with repositories: Running apt-get update is important because, without it, your system has no conceived idea as to whether updates are available for software available in your system; thereby vulnerable to numerous security risks or feature updates.

Ensures compatibility: The updated package lists are needed for other operations such as, updating packages or even installation of new packages with their dependencies.

2. sudo apt-get upgrade

The upgrade command is used to update all the package that is already installed on your system to their latest versions. It depends on the information that the update command collects.

What the Command Does:

Installs updated packages: This command if after running ‘apt-get update’ downloads new version of the installed packages if there is a newer version available.

Upgrades existing software: It updates the system replacing old package versions with the new ones but preserves the current settings.

Security patches: Most of the time this command helps to update important security patches and different bug fixes necessary for the system’s security and reliability.

Importance of Running upgrade:

Security: The upgrading makes sure that the parts that your system is made from has security fixes to some of the weaknesses that attackers can use. This is particularly necessary for servers, which are commonly attacked.

- Stability: Upgrades address issues which were specifically identified and pest the systems reliability and efficiency. This is important especially if the server provision has to be consistent.

- Performance improvements: New packages may have increased performance thus makes the system to run faster and more efficiently.

Why These Commands are Important:

- Security: These two commands are of, paramount importance in preventing unauthorized access to the server. VARs stated that there exists the need to patch software packages, the more so, if they are exposed to the internet (e.g., SSH, web server). If you have never run update and upgrade as a super user your system may be open to someone finding the known exploits.

- System health: Updating the system’s software will help it remain integrated, and run as desired by the system analysts and managers. Old packages may interfere with other software, or may contain certain bugs that would make them unreliable.

When should these commands be executed or how often should it be done?

- Regularly: As for me, these commands should be run on a daily basis, or at least on a weekly basis, especially on servers. For instance, to fit most production surroundings, it is advised that they be run on a weekly basis.

- Critical systems: Where security of data is paramount, or where ‘critical’ services reside, it remains advisable to automate these updates or run the updates more frequently such as once per day.

- Before installing new software: Before installing, please always type sudo apt-get update to check that you are being updated to the latest version to eliminate issues of dependencies.

From where do these commands pull the updates?

- Package repositories: The updates are obtained from repositories which, in simple terms are servers that contain packages and updates of various software. These repositories have Web addresses listed in /etc/apt/sources.list and the /etc/apt/sources.list.d/ directory.

For instance, sources for the update packages themselves are in the official Ubuntu repositories including archive.ubuntu.com.

You can also have additional repositories from third party sources for other software (for instance, Docker or Node.js).

1. **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)*

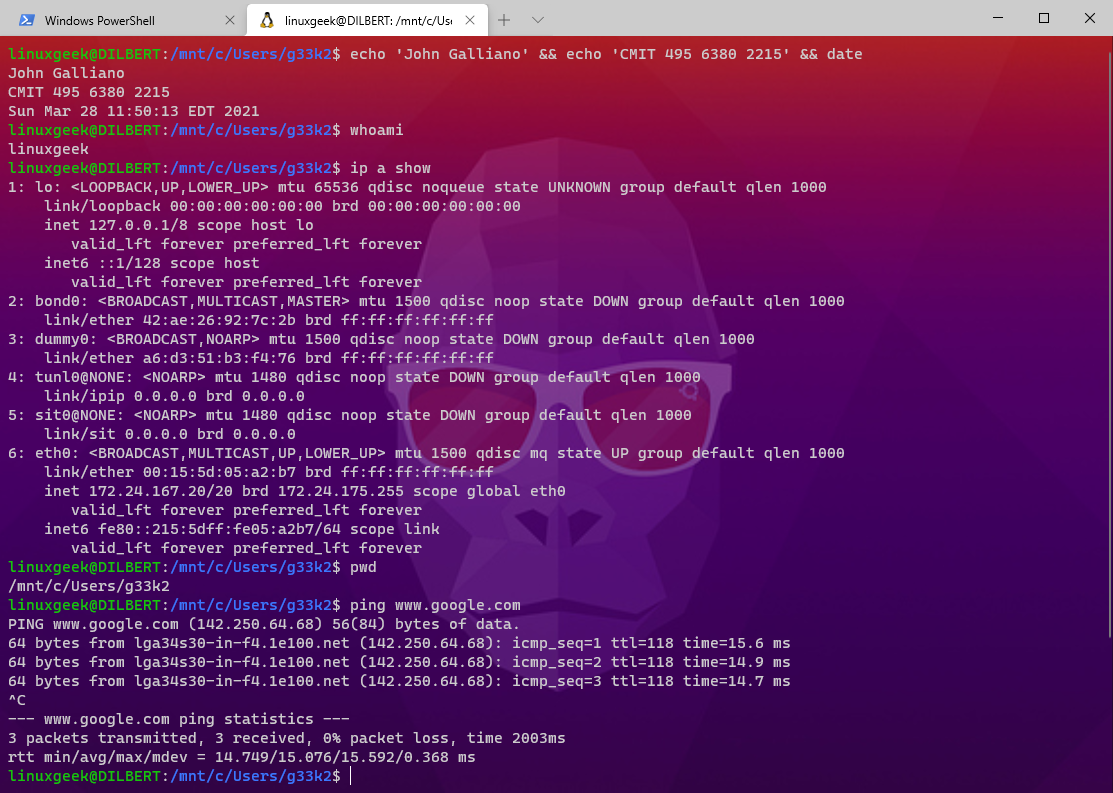
***whoami***

***ip***

***pwd***

**ping -c 4 www.google.com**

Example Screenshot:



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

If you type whoami it will show the user that is running the commands, in this case ubuntu. This shows you that you are logged into AWS as the default user that comes with the Ubuntu image.

1. **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.**

-Personal System (ipconfig): When the ipconfig has been entered in a personal system being it Windows or Linux the user is given the details of the network interfaces available on the device. The output also involves the IPv4 Address, which often as a private address, granted by the local router in the home or corporate network. It is identified as a private IP address on the IP address range, such as 192.168.x.x, 10.x.x.x or 172.16.x.x to 172.31.x.x from which cannot directly be accessed from the internet. The output used below also shows the Subnet Mask which is the part of the IP address that shows the network, and the Default Gateway which is the router IP address that directs traffic from the local network to the internet. By doing so, multiple PCs interconnected to the same local network in the home or office, bear one general IP address on the router that connects to the external networks.

-EC2 Instance (ip a show): The ip a show command inputs information about all the virtual network interfaces connected to the instance of the EC2. The output will normally consist of a public IP address and a private IP address, there is a possibility of receiving only one of them. The private IP address is given to the instance in AWS Virtual Private Cloud where the instance is created and uses numbers in the same range of numbers as used in local networks. This private address provides a direct connection between two instances instance located in the same VPC but also enables secure passage between two instances of the EC2 within the VPC. Furthermore, if the instance is configured for it, it comes with a public IP address assigned by AWS for Internet facing. This public IP enables user to gain access to the EC2 instance from any part of the world; thus, it is good for hosting web services or applications.

Differences in IP Addresses

The difference in the IP addresses, the one in the personal system and the another in the EC2 instance is due to the environment and usage. Your personal system usually connects with the Local Area Network (LAN) with a router assigning private IP address for interior communication. This private address is not directly accessible on the internet because the router has its different Internet protocol address by which outside connection is enabled. Surprisingly, the EC2 instance works within the cloud environment with the VPC configuration used as an organizational model. This implies that an instance has the internal IP address when the instances communicate to each other and an external IP address (if there is) from where users can access the instance from the internet. This means having both the public and private IPs in the cloud results in better networking but still has the protection of private addressing.

Published & Private IP Addresses

They are unique identifiers assigned to equipment that are require to communicate over internet and are globally routable IP’s. These addresses are assigned by Internet Service Providers (ISPs), or cloud service providers such as AWS and that can be reached by any device connected to the internet. For instance, a web server, with a web site, needs to have a PIP so that the permitted users can have access to the site from any part of the internet. Related to this, private IP addresses are used within LAN domains and have no possibility to be routed through the public Internet space. These are exclusive addresses that can be used in separate network without any problem due to their well-defined addresses (for instance 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255). Devices on the same LAN can use private IP addresses to communicate with each other but when they wish to connect to the internet, they have to send their packets through some device like a router with a public IP address. This separation also has the advantages of smooth networks and good security.

1. **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?**

Benefits of Virtualization in Data Center Consolidation

Virtualization is a big help in achieving data center convergence through allocating and managing multiple VMs on a single physical host, leading to efficiency and cost reduction in hardware purchases. Through this approach, unused servers are limited, thus reducing significantly the cases of costly investments in server equipment, as well as the expenses in powering and cooling them. As there are significantly fewer physical servers' organizations are benefitting from more effective management since the infrastructure is more compact and flexible; new VMs can be created in a short time to reflect changes in the business. In addition, virtualization simplifies disaster recovery and business continuity since VMs are easily duplicated and backed up so that a failure can be quickly recovered from. In summary, virtualization changes the character of data centers revolutionizing the IT infrastructure into more efficient, flexible and robust system.

Concerns During and After Transition

Consequently, virtualization provides diverse benefits when it comes to data center consolidation, but there also are a number of issues organizations should be concerned with before, during, and after the process. Resource sharing is one of the most threats because when many virtual machines are hosted on a single physical server, they may strive with other virtual machines for number of resources leading to poor performance. Also, virtualizing an environment might make it more difficult to manage, and this normally requires spending money on training and appropriate tools. There are security threats too; with a single hacked VM impacting others on the same host, protection must be strong against VM escaping and both require compliance with industry standards. In addition, organizations may be caught in a dilemma most often experienced in the form of vendor lock-in issues meaning that changing of strategies or technologies become difficult from the side of the organization. Lastly, the one time data migration process could be challenging due to the compatibility factor and possible downtime this makes it necessary to arrange and test for similar applications before a transfer is done.

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

Indeed, virtualization can greatly strengthen the security of an organization through several ways. Firstly, the virtualization technology offers better VM isolation giving a cleaner environment where should one of the VMs be compromised, it prevents inside movement to the rest of the network. They are used to maintain data and application’s privacy to avoid their contamination, modification or use by those not authorized. Secondly, virtualization can easily mean provision of security like firewalls, IT intrusion detections, and antivirus at the hypervisor level than it is in physical entity where traffic between VMs can be better controlled and monitored. Besides, through virtualization, new images or copies of VMs can be developed rapidly and in a secure manner than is possible with physical structure, and so little time is wasted in restoring the servers to a secure state in the event of a security break. Moreover, organizations can achieve segmentation by using virtual networks; to make sure that sensitive workloads are isolated from other less secure regions this makes it even more secure. Concisely, virtualization offers the improvement of flexibility and control, makes organizations seize the bull by the horns in terms of security while keeping efficiency.

1. **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?**

When analyzing the position of bare-metal (Type 1) and user-space (Type 2) hypervisors, it is seen that the bare-metal hypervisors are more secure. This is principally because they execute directly in the host hardware platform, and do not require an operating system on top of which they can be layered, thereby eliminating most of their surface area, that can be exploited by malicious elements. On the other hand, those hypervisors of Type 2 are launched as applications within a conventional operating system, and therefore they are as exposed to the flaws of the said host OS as any other application would be. It makes the security of all the VMs that run under the Type 2 hypervisor at risk in case the underlying operating system is hacked by attackers.

Vulnerabilities

Type 1 Hypervisors:

• Vulnerability to Hypervisor Attacks: While guest OSs have no direct access to or control of the Type 1 hypervisors, Type 1 hypervisors are also attacked by performing malicious hypervisor attacks that take advantage of hypervisor vulnerabilities. If an attacker manages to get into the ‘hypervisor layer’ they will be able to control all virtual machines running on that host.

• Configuration Risks: In another case, hypervisor misconfiguration or improper setup of hypervisor security measures can cause the problem and create a way for somebody to gain access to the VMs or to other pieces of information.

Type 2 Hypervisors:

• Dependency on Host OS: This is because Type 2 translators operate on top of a host OS; any vulnerability in the OS translates to entry to the hypervisor and VMs. This is because it deals with other malware for instance, malware that attacks the host OS.

• Resource Contention: It becomes a problem when resource contention such as CPU or memory usage affects the host OS which makes it challenging to apply security polices uniformly.

Mitigation Strategies

To mitigate the vulnerabilities associated with both types of hypervisors, organizations can implement several best practices:

1. Regular Updates and Patching: Make sure that all types of Hypervisors are updated and patched, also the Host Operating System (in case of Type II hypervisor).

2. Access Controls and Security Policies: Limit who may initiate commands to virtual hypervisors by authenticating the users and using roles and permissions to prohibit access to management interfaces. Use robust authentication techniques; the use of multiple form of authentications.

3. Network Segmentation: Apply network segmentation in order to clean different workloads and VMs from each other. This reduces the effect of a possible break in since if one of the VMs is compromised, the rest of the infrastructure cannot be easily penetrated.

4. Monitoring and Logging: Use strong monitoring and logging tools to identify novel events in the hypervisor environment. Commonly inspect log files in order to find signs of possible security threats.

5. Use of Security Tools: Upgrade systems protection by integration of IDS and antivirus solutions oriented to virtual environment.

6. Configuration Best Practices: Implement hypervisor conventional protocols of setting up and security. These include deactivation of unnecessary services, using hard configurations and firewall for traffic control at hypervisor level.

1. **Confirm that you have stopped and terminated your AWS Linux server instance. To confirm, simply type your name below.**

***Click or tap here to enter your name.***

1. *Link: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html* [↑](#footnote-ref-1)