

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

1. Creating a Linux Based Amazon Web Services (AWS) Instance
 - a. Go to your AWS Console, as seen in Figure 1.

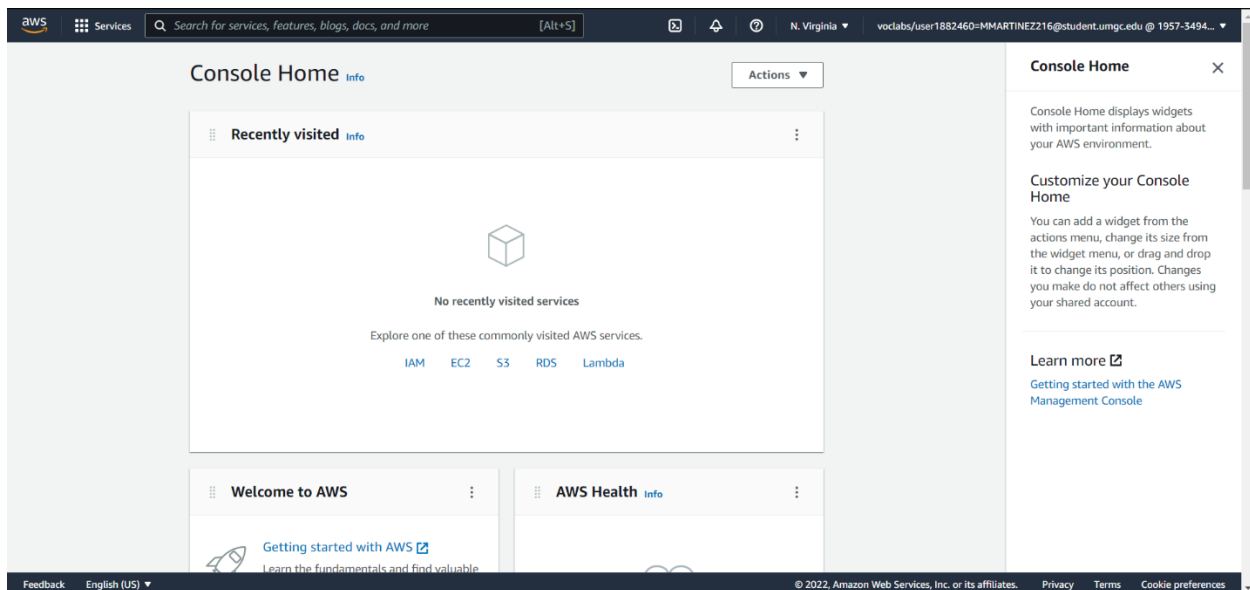


Figure 1: Amazon Web Services (AWS) Console

- b. Search for EC2 in the search bar at the top left of the screen, or scroll down to "Build a Solution," as seen in Figure 2. Then, click on "Launch a virtual machine."

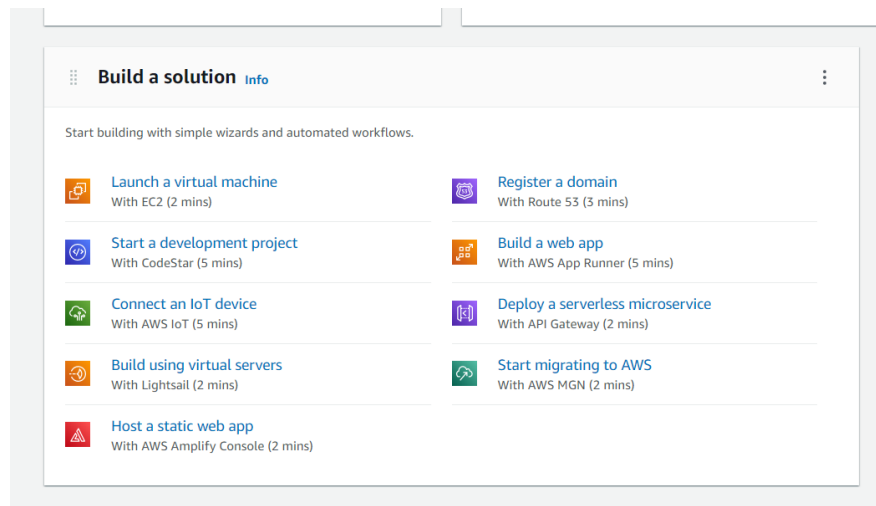


Figure 2: Start an EC2 Instance

- c. Choose your Operating System by clicking on the blue "Select" button. Figure 3 shows that this example uses "Ubuntu Server 20.04 LTS (HVM), SSD Volume Type; 64-bit (x86)."

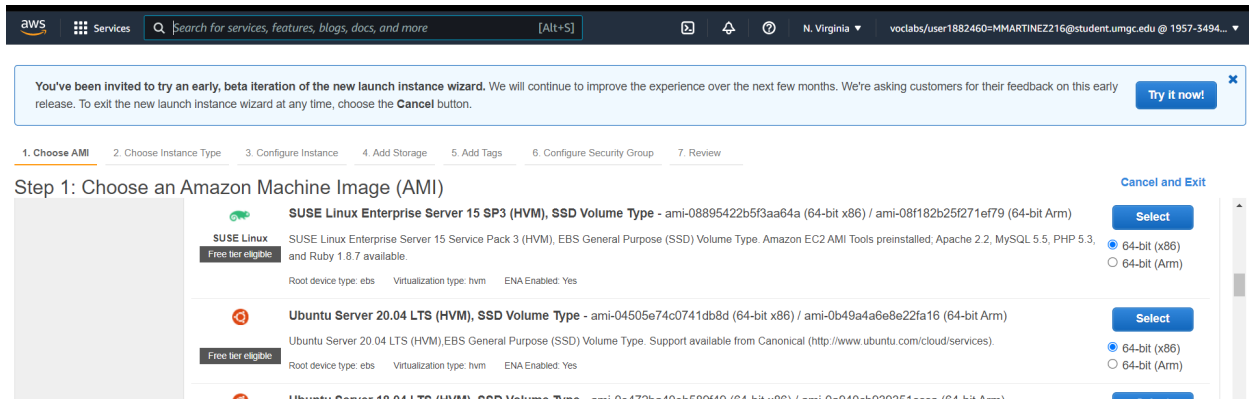


Figure 3: Choose the Operating System

- d. Choose the specifications for your Instance. AWS offers various specifications and allows you to choose a product that fits your needs. For example, as seen below, our Linux Server will use a "t2.micro" instance, which provides 1GB of memory with low to moderate network performance.
- e. Click on the blue "Review and Launch" button after you make a selection.

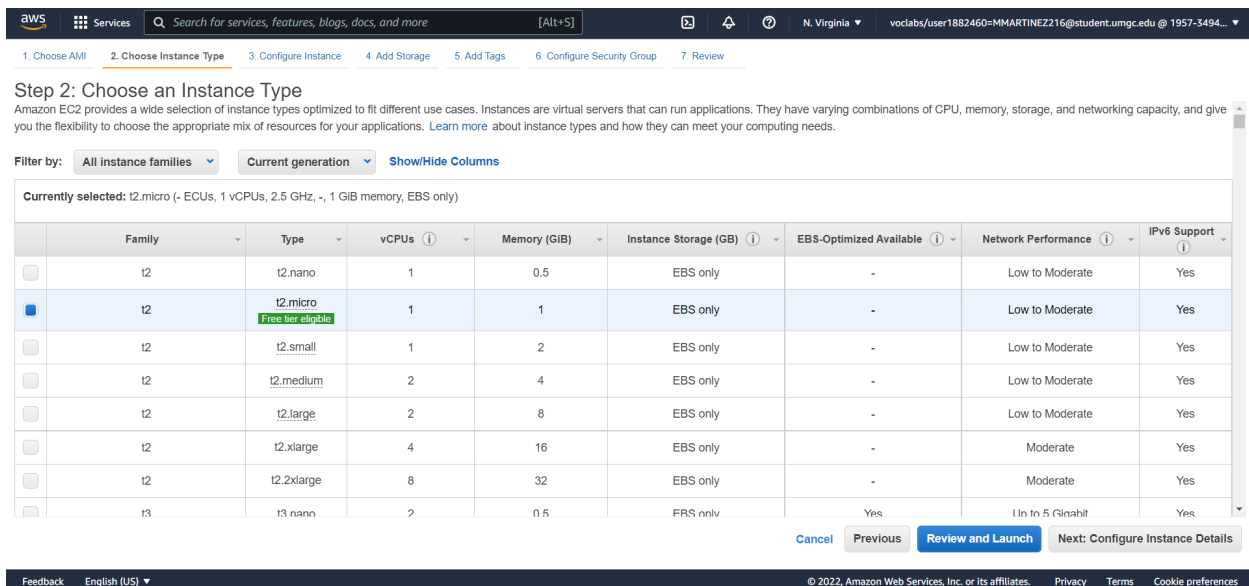


Figure 4: Choose specifications

- f. Click on the "Edit security groups" link, shown on the right-hand side of Figure 5, to configure the security group settings.

Step 7: Review Instance Launch

eligible: 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 2022-03-21T14:45:00.642+09:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

▶ Instance Details [Edit instance details](#)

▶ Storage [Edit storage](#)

▶ Tags [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

Figure 5: Configuring the Security Groups 1

- g. Create a new security group, or you choose an existing security group.
- h. Give your security group a unique name.
- i. Under the "Source" tab, click on the drop-down menu and select "My IP."
- j. Click on the blue "Review and Launch" button.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 110.70.50.226/32	e.g. SSH for Admin Desktop

[Add Rule](#)

[Cancel](#) [Previous](#) [Review and Launch](#)

Figure 6: Configuring the Security Groups 2

- k. Review your Instance to make sure all configurations are acceptable to your needs.
- l. Click on the blue "Launch" button.

Step 7: Review Instance Launch

eligible 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: Ubuntu SSH Martinez
Description: launch-wizard-1 created 2022-03-21T14:45:00.658+09:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	110.70.50.226/32	

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

[Cancel](#) [Previous](#) [Launch](#)

Figure 7: Confirm Configurations

- m. Select an existing key pair or create a new one.
- n. Give your key pair a unique name.
- o. Click on the "Download Key Pair" button and save the key pair to a safe location. Make sure you know where you downloaded the file; this file will **not** be able to be downloaded again after creation.
- p. Click on the blue "Launch Instances" button.

Step 7: Review Instance Launch

eligible Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)
t2.micro	-	1	1

Security Groups [Edit security groups](#)

Security group name: Ubuntu SSH Martinez
Description: launch-wizard-1 created 2022-03-21T14:45:00.658+09:00

Type	Protocol
SSH	TCP

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

[Cancel](#) [Previous](#) [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. Amazon EC2 supports ED25519 and RSA key pair types.

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](#).

Create a new key pair

Key pair type: ☒ RSA ☐ ED25519

Key pair name: CMIT495 Martinez

[Download Key Pair](#)

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

Figure 8: Create and Download a Key Pair

2. Using virtualization in a cloud environment helps to reduce IT expenditures (Shamir, 2021). When you are using virtualization, a single server can turn into multiple virtual machines running various operating systems and applications. This can maximize machine use and prevent idling and resources from being underutilized. In addition, if you use a cloud service instead of a physical machine, you cut costs further since you no longer provide physical upkeep.

Another benefit to using virtualization in a cloud environment is reduced downtime and enhanced disaster recovery (Shamir, 2021). With physical machines, if a disaster happens or the machine breaks down, it can take hours or even days to repair and recover the data or the machine itself. Virtualization allows for backups and other copies to quickly replace the affected virtual machine, bringing the downtime to minutes instead of days. In addition, when you add the cloud, servers are further protected since the virtual machine can have multiple copies and backups across large geographic regions. This will ensure that if a disaster takes down one server or region, one of the other regions can pick up the load and keep downtime to a minimum.

The third benefit of virtualization in a cloud environment is the amount of independence among the virtual machines (Shamir, 2021). Developers can quickly create a virtual environment to test new features or updates without affecting production. If an update or feature malfunctions and brings down the virtual machine, other virtual machines are independent enough to continue running.

3. Based on my experience launching this AWS Instance, the most challenging aspect is ensuring that the Instance will fit your needs. Setting it up is easy; however, some specifications need to be known before creation. For example, the operating system and the instance type are two properties of the Instance that needs to be known; otherwise, there can be issues with the virtual machine not meeting requirements.
4. Connect to the Ubuntu Server
 - a. Open the PuTTY Key Generator or equivalent program.
 - b. Click on the "load" button.
 - c. Select the key pair that was saved in step 1o.
 - d. Click "Save private key" and then click "Yes."

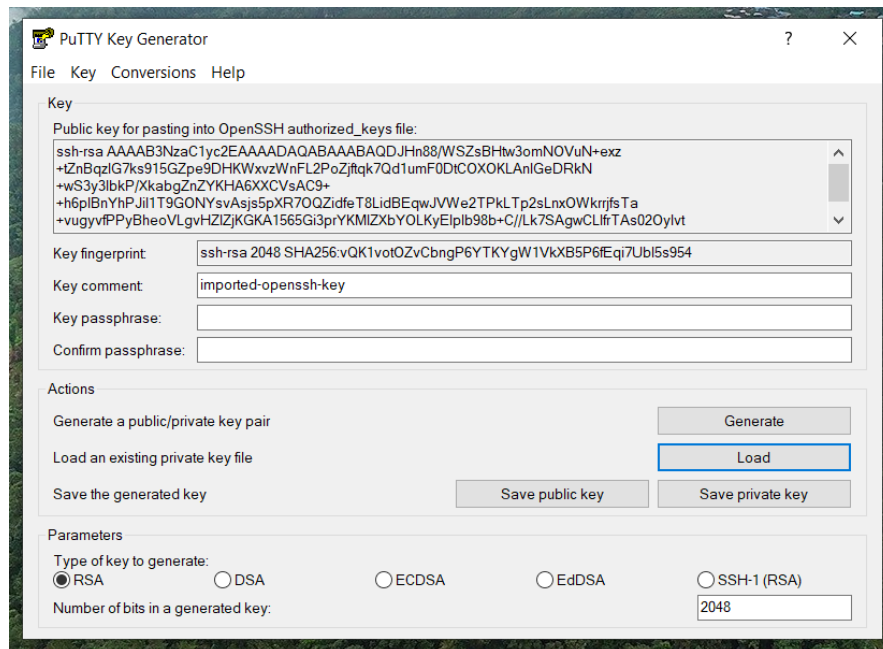


Figure 9: Creating a Usable Key

- e. Open PuTTY.
- f. Type "ubuntu@[IP address of Ubuntu server]" in the "Host Name (or IP address)" box.

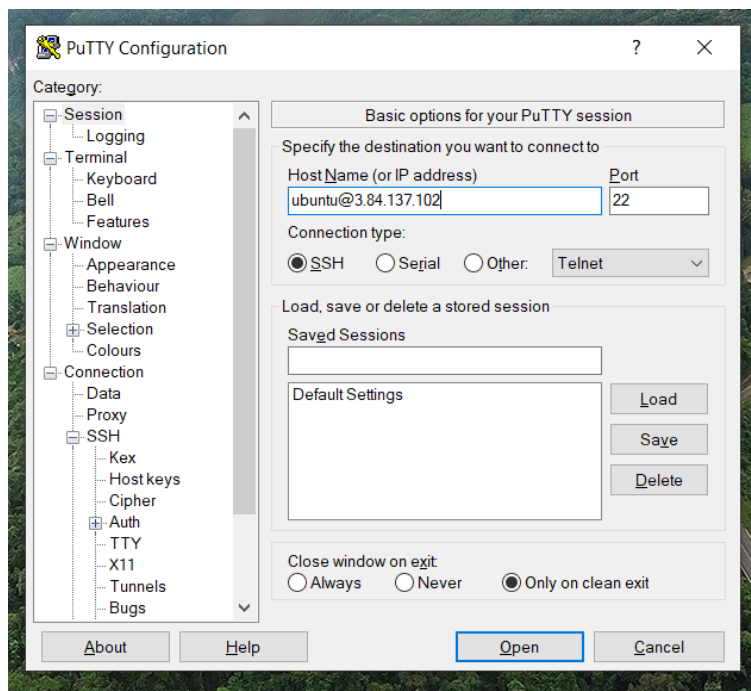


Figure 10: PuTTY Home Screen

- g. Click on the "Connection" tab on the left-hand side.
- h. Click on the "+" sign next to "SSH."
- i. Click on "Auth."
- j. Select the "Browse" button and load the Private Key saved in step 4d.

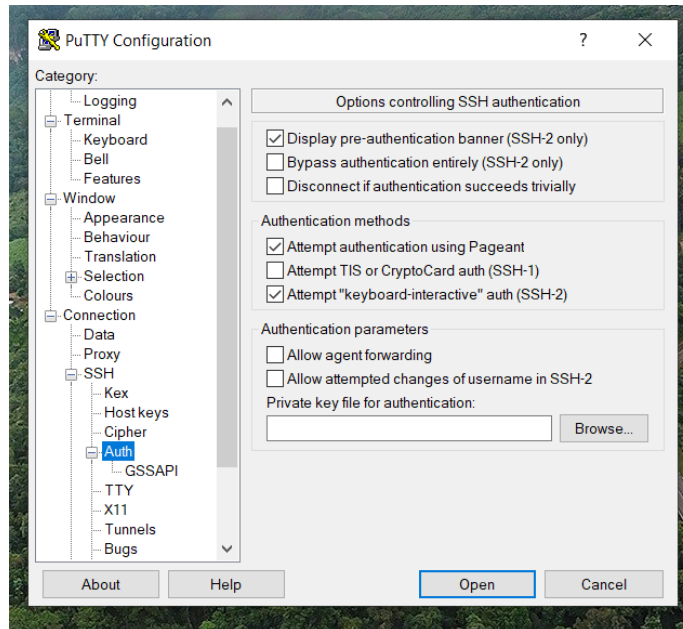


Figure 11: PuTTY Authentication Settings

- k. Click "Open" to connect to the Ubuntu Server.

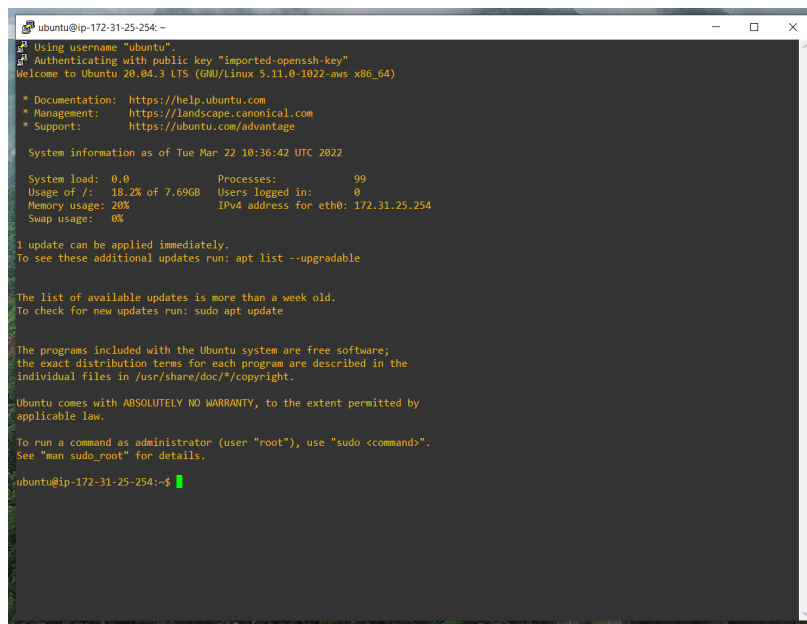
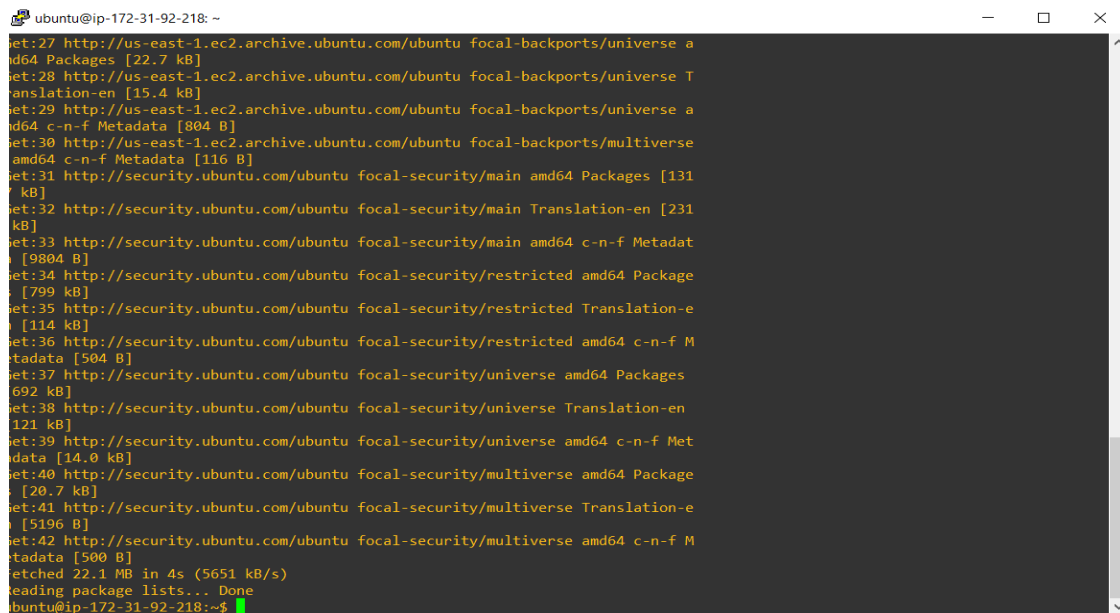
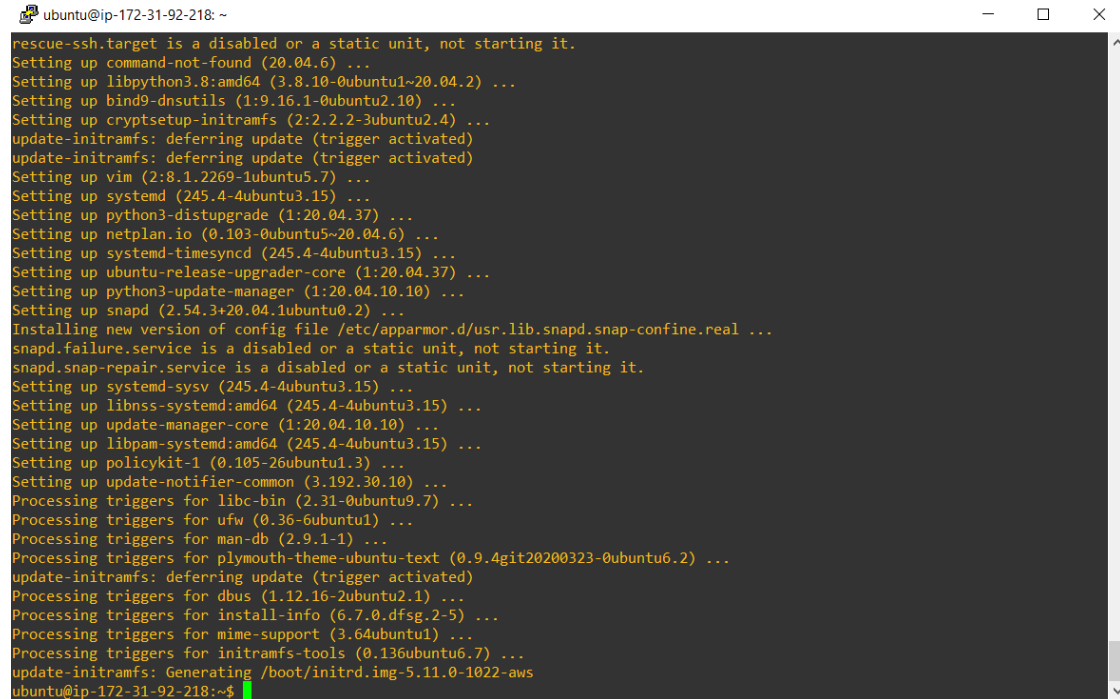


Figure 12: Successful Logon

5. Update your Linux Server using "*sudo apt-get update*" and "*sudo apt-get upgrade*."

```
ubuntu@ip-172-31-92-218: ~  
get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports/universe a  
md64 Packages [22.7 kB]  
get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports/universe T  
ranslation-en [15.4 kB]  
get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports/universe a  
md64 c-n-f Metadata [804 B]  
get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports/multiverse  
amd64 c-n-f Metadata [116 B]  
get:31 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [131  
kB]  
get:32 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [231  
kB]  
get:33 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadat  
a [9804 B]  
get:34 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Package  
s [799 kB]  
get:35 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-e  
n [114 kB]  
get:36 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f M  
etadata [504 B]  
get:37 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages  
692 kB]  
get:38 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en  
121 kB]  
get:39 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Met  
adata [14.0 kB]  
get:40 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Package  
s [20.7 kB]  
get:41 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-e  
n [5196 B]  
get:42 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f M  
etadata [500 B]  
etched 22.1 MB in 4s (5651 kB/s)  
reading package lists... Done  
ubuntu@ip-172-31-92-218:~$
```

Figure 13: Successful "*sudo apt-get update*" command

```
ubuntu@ip-172-31-92-218: ~  
rescue-ssh.target is a disabled or a static unit, not starting it.  
Setting up command-not-found (20.04.6) ...  
Setting up libpython3.8:amd64 (3.8.10-0ubuntu1~20.04.2) ...  
Setting up bind9-dnssutils (1:9.16.1-0ubuntu2.10) ...  
Setting up cryptsetup-initramfs (2:2.2.2-3ubuntu2.4) ...  
update-initramfs: deferring update (trigger activated)  
update-initramfs: deferring update (trigger activated)  
Setting up vim (2:8.1.2269-1ubuntu5.7) ...  
Setting up systemd (245.4-4ubuntu3.15) ...  
Setting up python3-distupgrader (1:20.04.37) ...  
Setting up netplan.io (0.103-0ubuntu5~20.04.6) ...  
Setting up systemd-timesyncd (245.4-4ubuntu3.15) ...  
Setting up ubuntu-release-upgrader-core (1:20.04.37) ...  
Setting up python3-update-manager (1:20.04.10.10) ...  
Setting up snapd (2.54.3+20.04.1ubuntu0.2) ...  
Installing new version of config file /etc/apparmor.d/usr.lib.snapd.snap-confine.real ...  
snapd.failure.service is a disabled or a static unit, not starting it.  
snapd.snap-repair.service is a disabled or a static unit, not starting it.  
Setting up systemd-sysv (245.4-4ubuntu3.15) ...  
Setting up libnss-systemd:amd64 (245.4-4ubuntu3.15) ...  
Setting up update-manager-core (1:20.04.10.10) ...  
Setting up libpam-systemd:amd64 (245.4-4ubuntu3.15) ...  
Setting up policykit-1 (0.105-26ubuntu1.3) ...  
Setting up update-notifier-common (3.192.30.10) ...  
Processing triggers for libc-bin (2.31-0ubuntu9.7) ...  
Processing triggers for ufw (0.36-6ubuntu1) ...  
Processing triggers for man-db (2.9.1-1) ...  
Processing triggers for plymouth-theme-ubuntu-text (0.9.4git20200323-0ubuntu6.2) ...  
update-initramfs: deferring update (trigger activated)  
Processing triggers for dbus (1.12.16-2ubuntu2.1) ...  
Processing triggers for install-info (6.7.0.dfsg.2-5) ...  
Processing triggers for mime-support (3.64ubuntu1) ...  
Processing triggers for initramfs-tools (0.136ubuntu6.7) ...  
update-initramfs: Generating /boot/initrd.img-5.11.0-1022-aws  
ubuntu@ip-172-31-92-218:~$
```

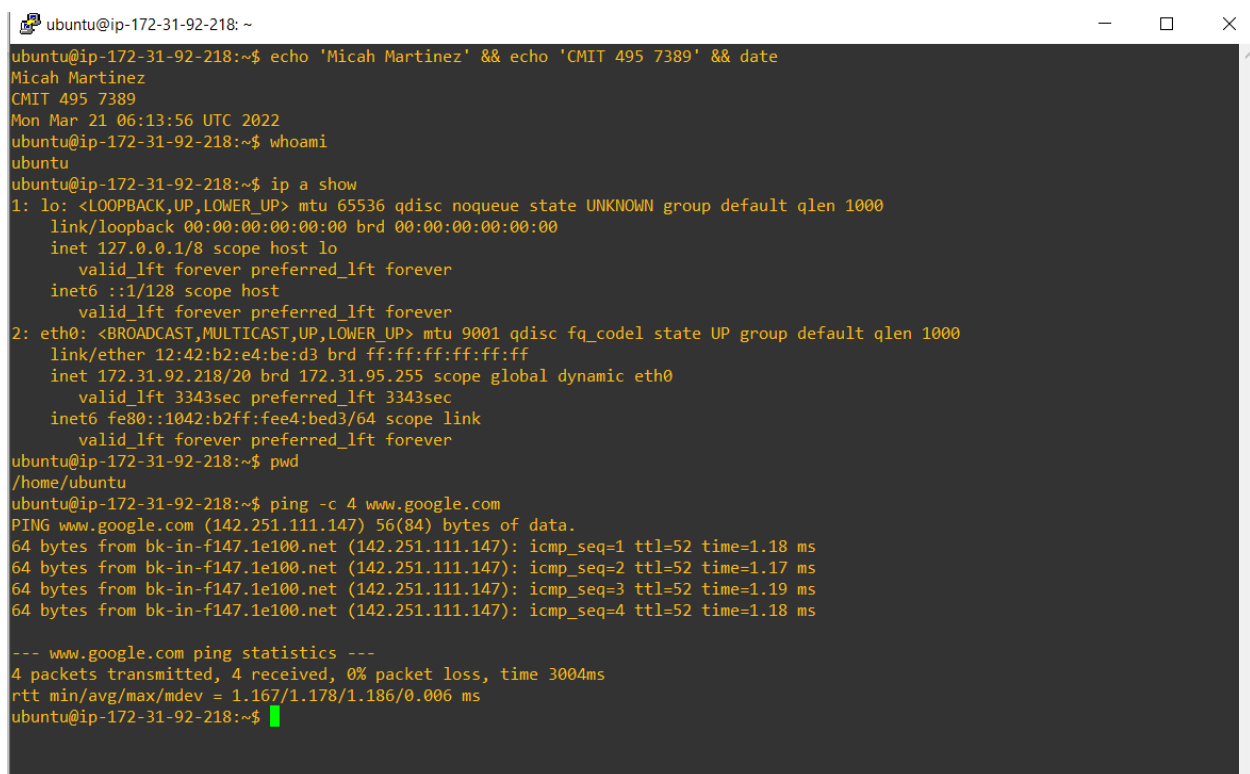
Figure 14: Successful "*sudo apt-get upgrade*" command

- The `"sudo apt-get update"` command downloads package information from all configured sources (Gite, 2022). These sources are usually found in the `"/etc/apt/sources.list"` file and the `"/etc/apt/sources.list.d/"` directory. So, when you run this command, you download updated package information from the Internet.

The `"sudo apt-get upgrade"` command is the command that installs these new updates. Therefore, all available upgrades found by the `"sudo apt-get update"` command will be installed. Because of this, the update command must be run before the upgrade command.

One nice thing about Ubuntu is that it is automatically configured to run the update command about once a week (AskUbuntu, 2013), which is generally a good timeframe to run these commands. After it runs this command, it will allow you to pick and choose which packages you want to install. However, you can change this configuration in the settings to run the update and upgrade commands at different intervals of your choosing.

7. System Information

A terminal window titled 'ubuntu@ip-172-31-92-218: ~' with standard window controls. The terminal shows the following commands and output:

```
ubuntu@ip-172-31-92-218:~$ echo 'Micah Martinez' && echo 'CMIT 495 7389' && date
Micah Martinez
CMIT 495 7389
Mon Mar 21 06:13:56 UTC 2022
ubuntu@ip-172-31-92-218:~$ whoami
ubuntu
ubuntu@ip-172-31-92-218:~$ ip a show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 12:42:b2:e4:be:d3 brd ff:ff:ff:ff:ff:ff
    inet 172.31.92.218/20 brd 172.31.95.255 scope global dynamic eth0
        valid_lft 3343sec preferred_lft 3343sec
    inet6 fe80::1042:b2ff:fee4:bed3/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@ip-172-31-92-218:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-92-218:~$ ping -c 4 www.google.com
PING www.google.com (142.251.111.147) 56(84) bytes of data.
64 bytes from bk-in-f147.1e100.net (142.251.111.147): icmp_seq=1 ttl=52 time=1.18 ms
64 bytes from bk-in-f147.1e100.net (142.251.111.147): icmp_seq=2 ttl=52 time=1.17 ms
64 bytes from bk-in-f147.1e100.net (142.251.111.147): icmp_seq=3 ttl=52 time=1.19 ms
64 bytes from bk-in-f147.1e100.net (142.251.111.147): icmp_seq=4 ttl=52 time=1.18 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.167/1.178/1.186/0.006 ms
ubuntu@ip-172-31-92-218:~$
```

Figure 15: System Information

- The `"whoami"` command is used to find the username of the account that is in use (Mlynarik, 2020). For example, Figure 15 shows that our current username is "ubuntu." This

is most likely just a standard user. If we were using the root account, it would have returned "root" instead of "ubuntu."

9. The main difference between the IP address on the Linux system and the IP address on my personal system is that the Linux IP address is class B, and my personal IP address is a class C. These IP addresses are different because of the size of the network they are on. Class B addresses are generally used for medium-sized networks, while class C addresses are used for small networks (Tech Target, 2020).

Both IP addresses are in the "private IP address range" (IBM, 2022). Private IP addresses are not unique and are considered non-routable; this allows businesses to use them within their private network, in any way they see fit, without the public having access to them. Public addresses are unique, can be accessed directly through the Internet, and are assigned by the internet provider.

10. Virtualization could help a data center consolidate by bringing down material and upkeep costs. In addition, data centers likely have many physical servers that are used in multiple locations. By transitioning to virtual servers, they can remove those physical servers freeing up physical space and possibly removing buildings that previously housed servers. However, I would be leery about a hasty transition resulting in data loss. If the data center implements the change without backups or a transition plan, lots of data can be lost. There may also be issues with employees not understanding how to access resources. The transition must allow software compatibility with the old system so that employees do not have to be retrained or new software needs to be added.
11. Virtualization generally has little to no effect on the security of a system (Scarfone et al., 2011). It has been found that if a service or a resource has a vulnerability, virtualization will not remedy that vulnerability. Virtualization limits the effects of possible exploitation due to the independence and recovery capabilities mentioned earlier.
12. Native (type 1) hypervisors tend to be more secure. This is because type 1 hypervisors do not rely on an underlying Operating System (OS), which means that they do not have the flaws and vulnerabilities that come with the OS (Reseller Club, 2019). Unfortunately, this leads to what I believe is one of the most significant vulnerabilities of type 2 hypervisors, the OS they rely upon. In addition, having multiple virtual machines running off a single OS provides a common link among the virtual machines. Therefore, if the OS is successfully exploited, the virtual machines are also in danger of being exploited. To secure this weakness, ensure that the OS has is hardened as much as possible, known vulnerabilities have been patched, and is continually updated.

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

Micah L Martinez

References

- AskUbuntu. (2013, September 11). *How often should I update using apt-get update?* Retrieved from AskUbuntu: <https://askubuntu.com/questions/344352/how-often-should-i-update-using-apt-get-update#:~:text=In%20your%20case%20you%20would,downloads%2Finstalls%20the%20selected%20ones.>
- Gite, V. (2022, February 5). *What does sudo apt-get update command do on Ubuntu/Debian?* Retrieved from CyberCiti: <https://www.cyberciti.biz/faq/what-does-sudo-apt-get-update-command-do-on-ubuntu-debian/>
- IBM. (2022, January 17). *Private Address Ranges*. Retrieved from IBM: <https://www.ibm.com/docs/en/networkmanager/4.2.0?topic=translation-private-address-ranges>
- Mlynarik, R. (2020, March). *Whoami*. Retrieved from man7: <https://man7.org/linux/man-pages/man1/whoami.1.html>
- Reseller Club. (2019, May 24). *Type 1 and Type 2 Hypervisors: What Makes Them Different*. Retrieved from Medium: <https://medium.com/teamresellerclub/type-1-and-type-2-hypervisors-what-makes-them-different-6a1755d6ae2c>
- Scarfone, K., Souppaya, M., & Hoffman, P. (2011) National Institute of Standards and Technology (NIST) Special Publication 800-125: Guide to security for full virtualization techniques. <https://doi.org/10.6028/NIST.SP.800-125>
- Shamir, J. (2021, April 8). *5 Benefits of Virtualization*. Retrieved from IBM: <https://www.ibm.com/cloud/blog/5-benefits-of-virtualization>
- Tech Target. (2020, October). *IPv4 address class*. Retrieved from Tech Target: <https://whatis.techtarget.com/definition/IPv4-address-class>