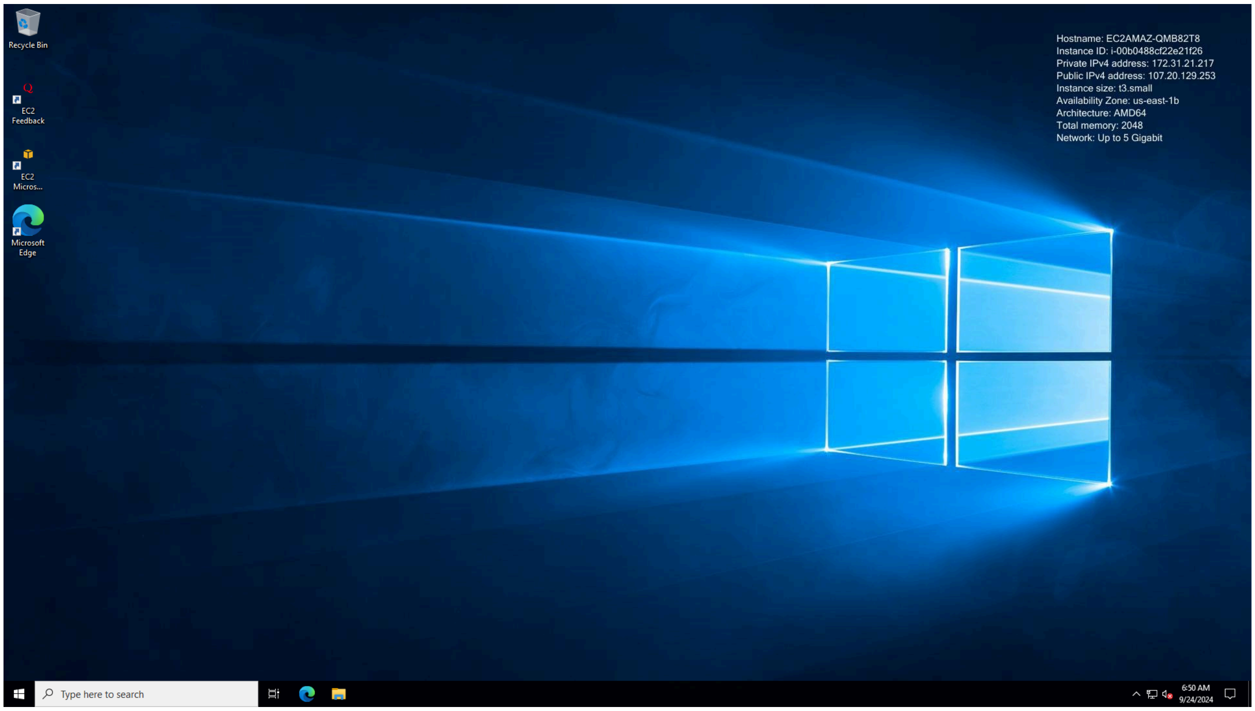
CIS 2650

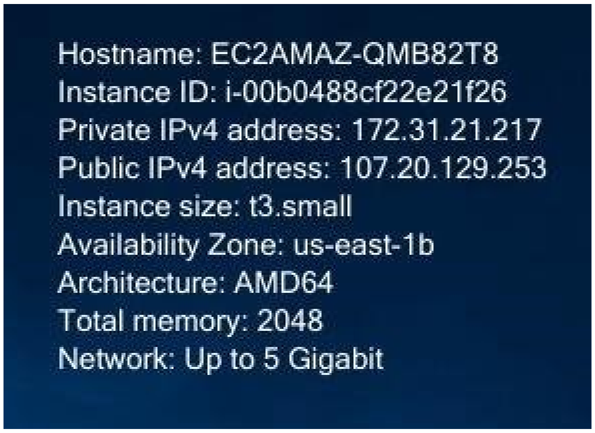
Assignment 1

Windows Server Creation and Connection

Screenshot 1 – Windows RDP Connection



Hostname: EC2AMAZ-QMB82T8
Instance ID: i-00b0488cf22e21f26
Private IPv4 address: 172.31.21.217
Public IPv4 address: 107.20.129.253
Instance size: t3.small
Availability Zone: us-east-1b
Architecture: AMD64
Total memory: 2048
Network: Up to 5 Gigabit



Hostname: EC2AMAZ-QMB82T8
Instance ID: i-00b0488cf22e21f26
Private IPv4 address: 172.31.21.217
Public IPv4 address: 107.20.129.253
Instance size: t3.small
Availability Zone: us-east-1b
Architecture: AMD64
Total memory: 2048
Network: Up to 5 Gigabit

(it was hard due to my resolution to make that visible)

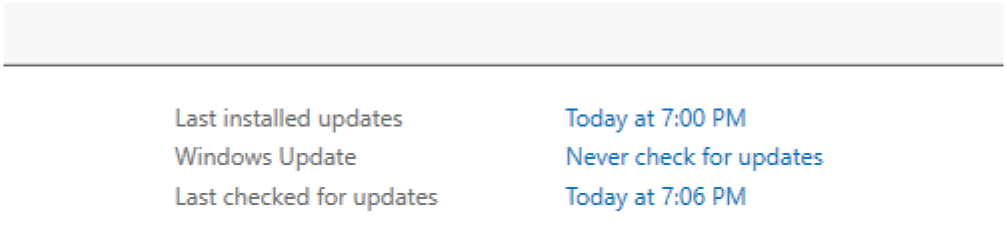
Question 1: What AWS instance size did you use and what resources does that provide to your Windows virtual machine?

A:

- *Instance Size:*
  - ***t3.small***
- *RAM:*
  - ***1.96 (2GB)***
- *Hard disk space:*
  - ***29.9 GB (30 GB)***
- *Physical CPUs:*
  - ***1 Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz   2.50 GHz***
- *CPU Cores:*
  - ***2 virtual processors***

Installing Windows Updates

Screenshot 2 – Windows Updates Performed

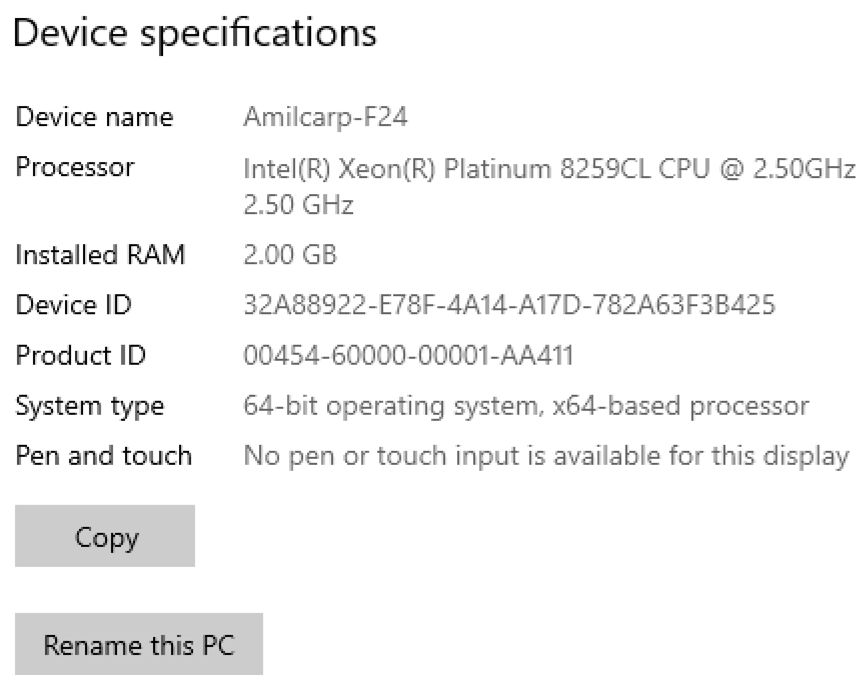


Last installed updates	Today at 7:00 PM
Windows Update	Never check for updates
Last checked for updates	Today at 7:06 PM

(I kept checking and even rebooted yet it did not change)

Windows Computer Name

Screenshot 3 – Changed Computer Name



Device specifications

Device name	Amilcarp-F24
Processor	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2.50 GHz
Installed RAM	2.00 GB
Device ID	32A88922-E78F-4A14-A17D-782A63F3B425
Product ID	00454-60000-00001-AA411
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

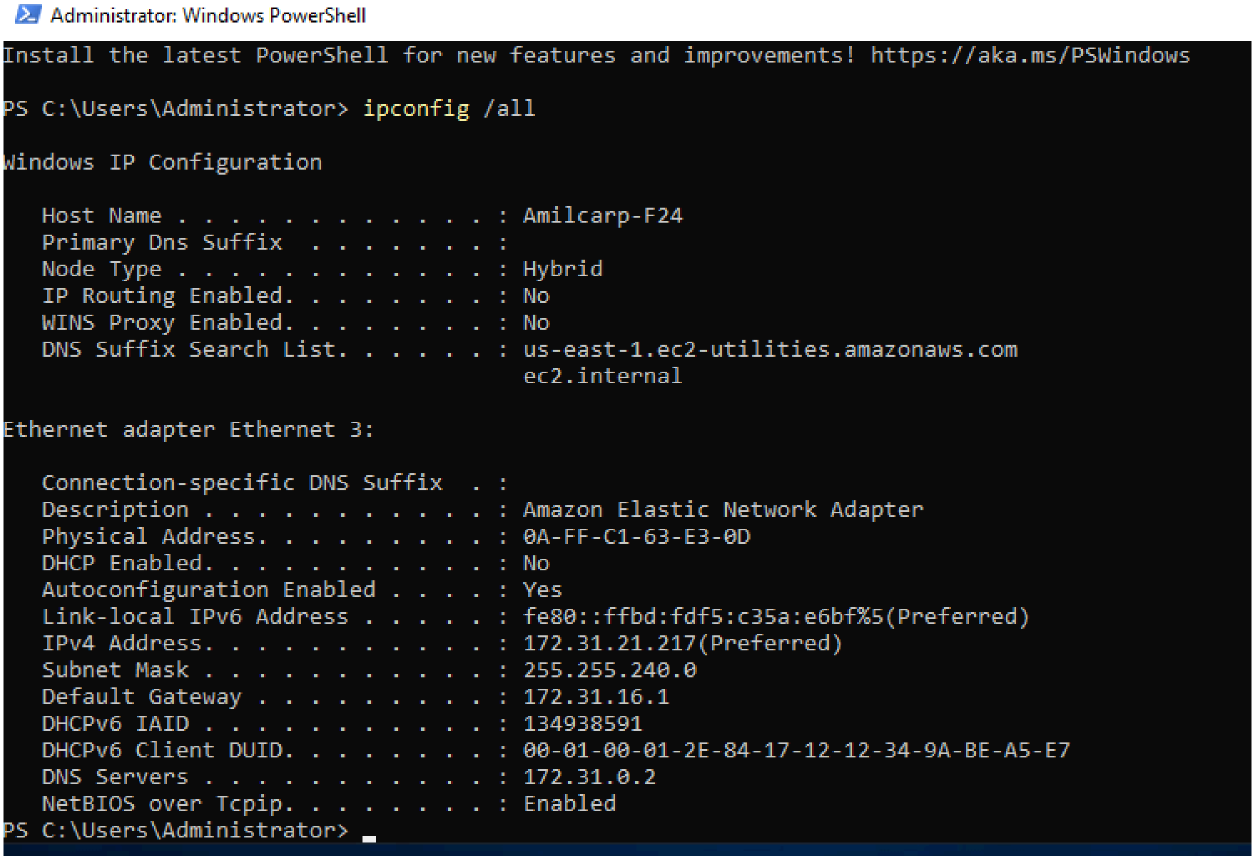
Question 2: Write two to three paragraphs that describes Microsoft’s patch release cycle (e.g. when are they released, what happens if there is a super critical patch, etc.) and the importance of keeping your servers up to date on a regular basis from a security and a reliability perspective.

A: Microsoft has a regular schedule on the 2nd tuesday of every month for their patch releases. It is mainly known as patch tuesday due to this and lets people in IT anticipate in accordance to the update and plan for the update. But there is times when there is a huge vulnerability that has been found and can pose a huge threat. When this happens microsoft releases a out of band update outside of the schedule in order to address these possibly critical issues like as we mentioned zero day vulnerabilities in order to patch them as soon as possible to prevent system compromisations.

The importance of keeping servers up to date is critical for security and reliability. Security wise its needed because the updates patch up the system where there can be prime vulnerabilities protecting them from cyber attacks. This means that the outdated software can have exploitable weaknesses but regular patching helps close these vulnerabilities before they can be exploited reducing the attackers chances. However from a reliability standpoint it also addresses bugs and performances enhancement. This helps servers operate without any problems and make sure they don't stay down for long enhancing the experience of everyone.

Static IP Address Assignment

Screenshot 4 – Statically Assigned IP Address



```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Amilcarp-F24
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : us-east-1.ec2-utilities.amazonaws.com
                                       ec2.internal

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter
   Physical Address. . . . . . . . . : 0A-FF-C1-63-E3-0D
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ffbd:fdf5:c35a:e6bf%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.31.21.217(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.16.1
   DHCPv6 IAID . . . . . . . . . . . : 134938591
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-84-17-12-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 172.31.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\Administrator> _
```

Windows Information Output

From the data in the output from msinfo32 answer the following:

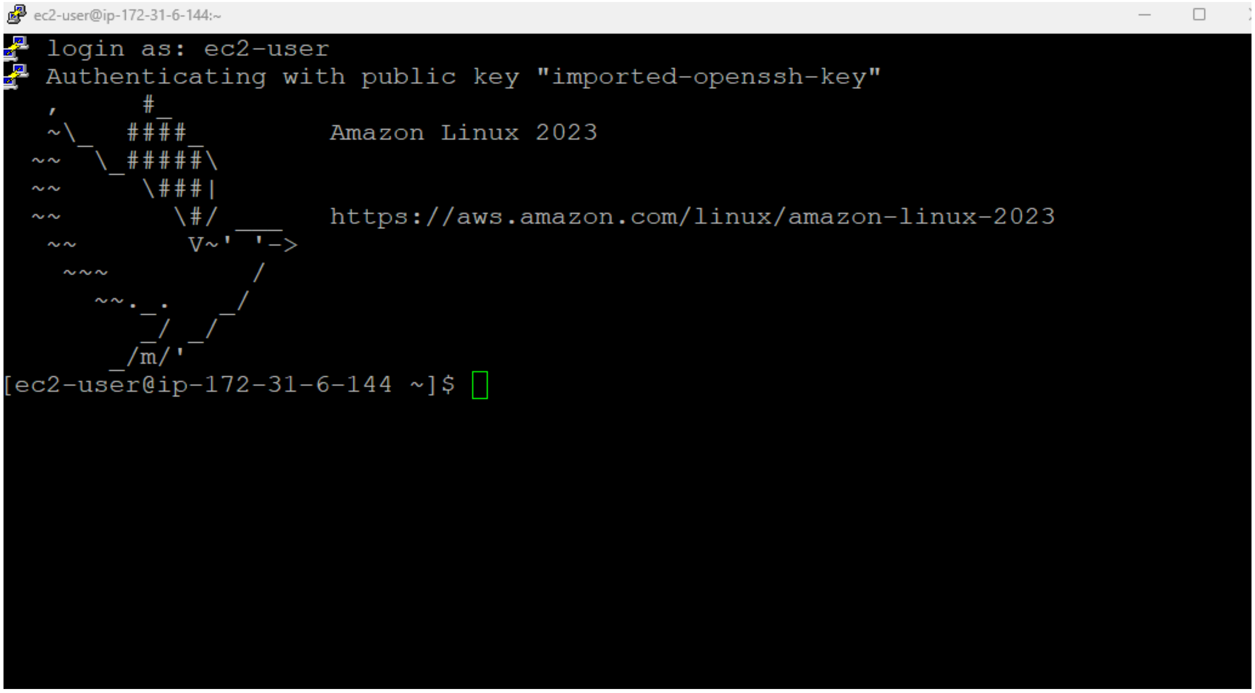
Question 3: From the data in the output from msinfo32:

A:

- *How many and what type of processors does your server have?*
    - ***Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 2500 Mhz, 1 Core(s), 2 Logical Processor(s)***
- How much physical memory does your virtual machine have installed?
    - ***Installed Physical Memory (RAM)   2.00 GB***
- How much physical memory does your virtual machine have available?
    - ***Available Physical Memory   622 MB***
- What is the exact version number of the Windows Server installation?
    - ***Version 10.0.20348 Build 20348***
- What is the BIOS version and date?
    - ***Amazon EC2 1.0, 10/16/2017***

Linux Server Creation and Connection

Screenshot 5 – Linux SSH Connection



```
   login as: ec2-user
   Authenticating with public key "imported-openssh-key"
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-6-144 ~]$
```

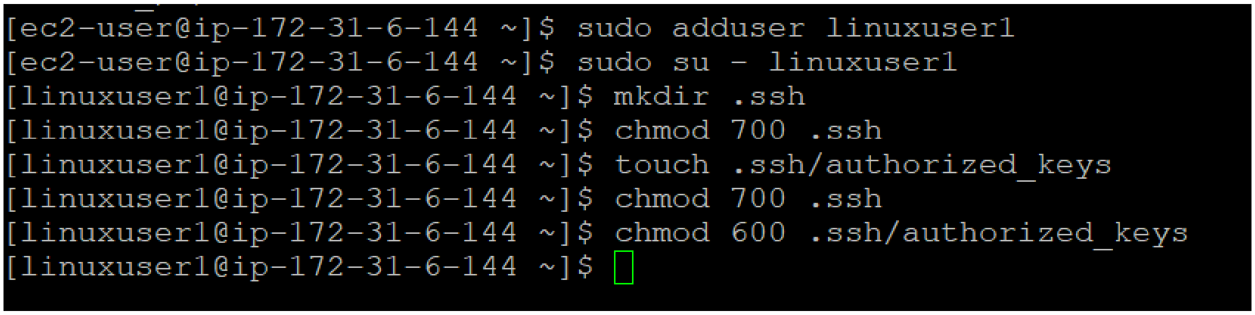
Question 4: What AWS instance size did you use and what resources does that provide to your Linux virtual machine?

A:

- *Instance Size:*
  - **t2.micro**
- *RAM:*
  - **949 Mi**
- *Hard disk space:*
  - **8 GB**
- *Physical CPUs:*
  - **1**
- *CPU Cores:*
  - **1**

Add a Linux User

Screenshot 6 – Adding User



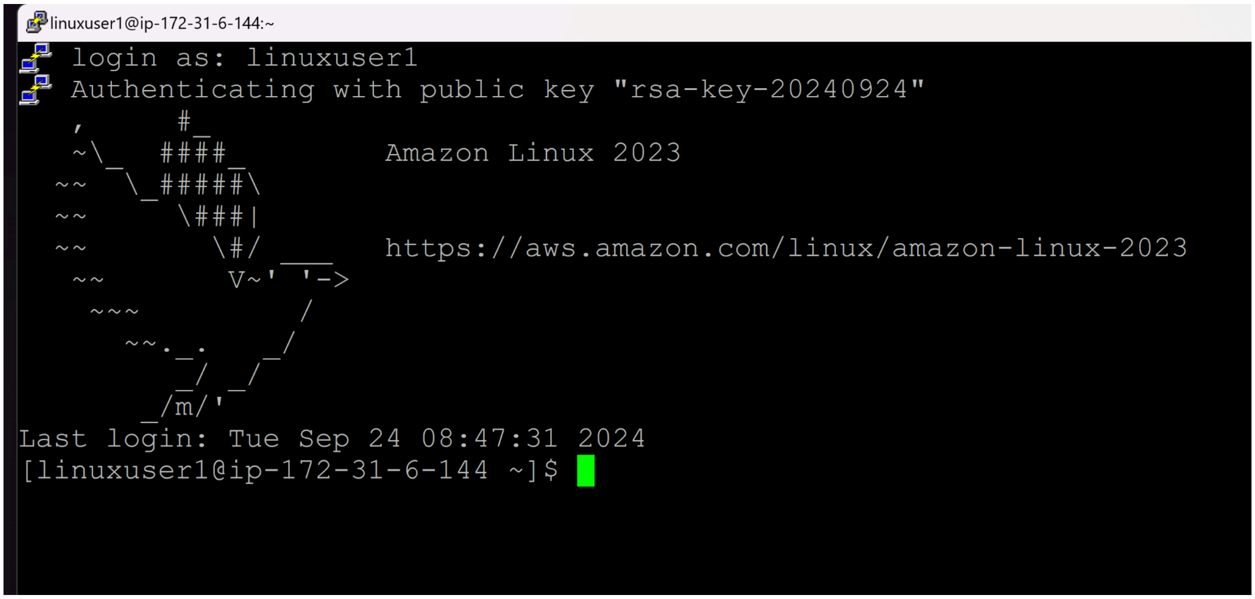
```
[ec2-user@ip-172-31-6-144 ~]$ sudo adduser linuxuser1
[ec2-user@ip-172-31-6-144 ~]$ sudo su - linuxuser1
[linuxuser1@ip-172-31-6-144 ~]$ mkdir .ssh
[linuxuser1@ip-172-31-6-144 ~]$ chmod 700 .ssh
[linuxuser1@ip-172-31-6-144 ~]$ touch .ssh/authorized_keys
[linuxuser1@ip-172-31-6-144 ~]$ chmod 700 .ssh
[linuxuser1@ip-172-31-6-144 ~]$ chmod 600 .ssh/authorized_keys
[linuxuser1@ip-172-31-6-144 ~]$ 
```

Question 5: In this assignment we are using ssh keys for authentication. Linux also supports authenticating using a username/password combination. In two to three paragraphs, describe the pros and cons of using these two authentication methods.

A: ***The two common methods of SSH keys and user/passwords is common practice on linux in way that we practiced of having the SSH private key on our device connect the the server through the public copy that it has. When other people trying to attempt to authenticate the server uses the public key to make sure that the private key is valid and is used because it enhances the security. Without that private key there is no way to get in due to it not being able to validate due to the public key not seeing its private key counter part. This helps especially in the field of phishing attackers since its harder to get it due to it not being something like a password since it never leaves the primary system.***

Username nad passwords is simpler to set up and easier for basic users who don't know what a SSH key is as they are not network admins since it doesn't need special programs just a USERNAME and a good password like 123456. However this comes with security risks as the mentioned phishing attacks can get ahold of the username and amazing 123456 password and then be used to login pretending to be the user that username and password combination was meant for. This is especially annoying when there is work environments where the password must be changed every quarter and cant be the same thing with notable differences and or requirements. In general SSH combo is safer and better but is harder to set up and requires actual knowledge while username/password is easier to use and safe however its biggest fault is the people itself making security worse and not comparable to SSH.

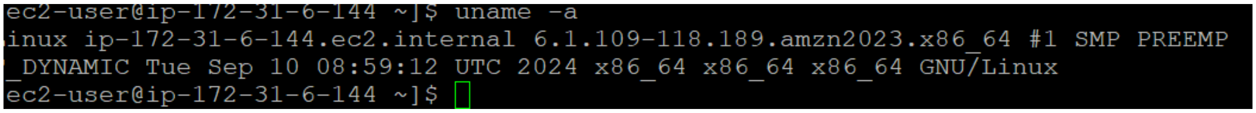
Screenshot 7 – Log in with New User



```
login as: linuxuser1
Authenticating with public key "rsa-key-20240924"
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Tue Sep 24 08:47:31 2024
[linuxuser1@ip-172-31-6-144 ~]$
```

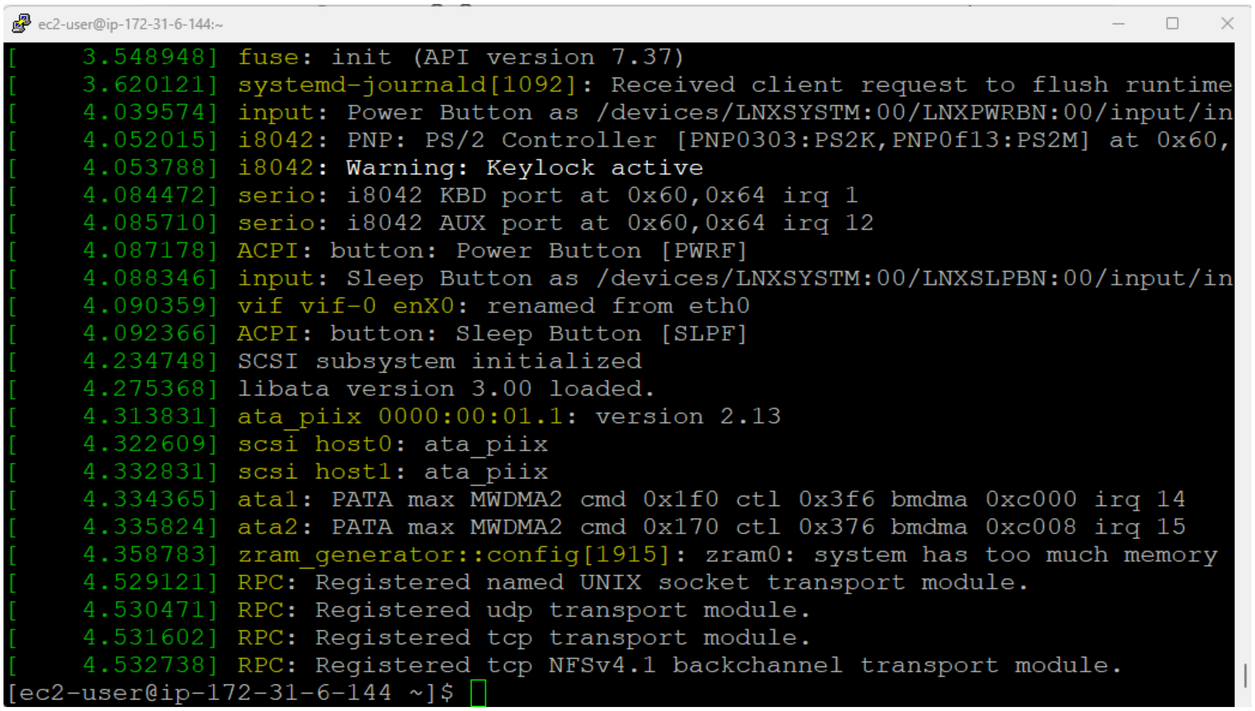
Linux Command Output

Screenshot 8 – Command (uname -a)



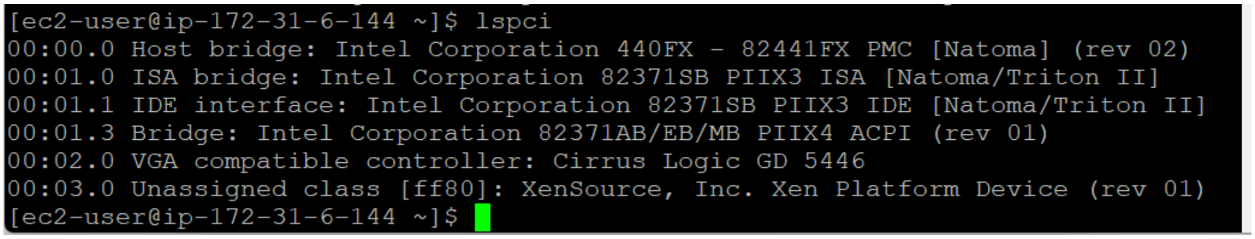
```
ec2-user@ip-172-31-6-144 ~]$ uname -a
inux ip-172-31-6-144.ec2.internal 6.1.109-118.189.amzn2023.x86_64 #1 SMP PREEMP
_DYNAMIC Tue Sep 10 08:59:12 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 9 – Command (dmesg)



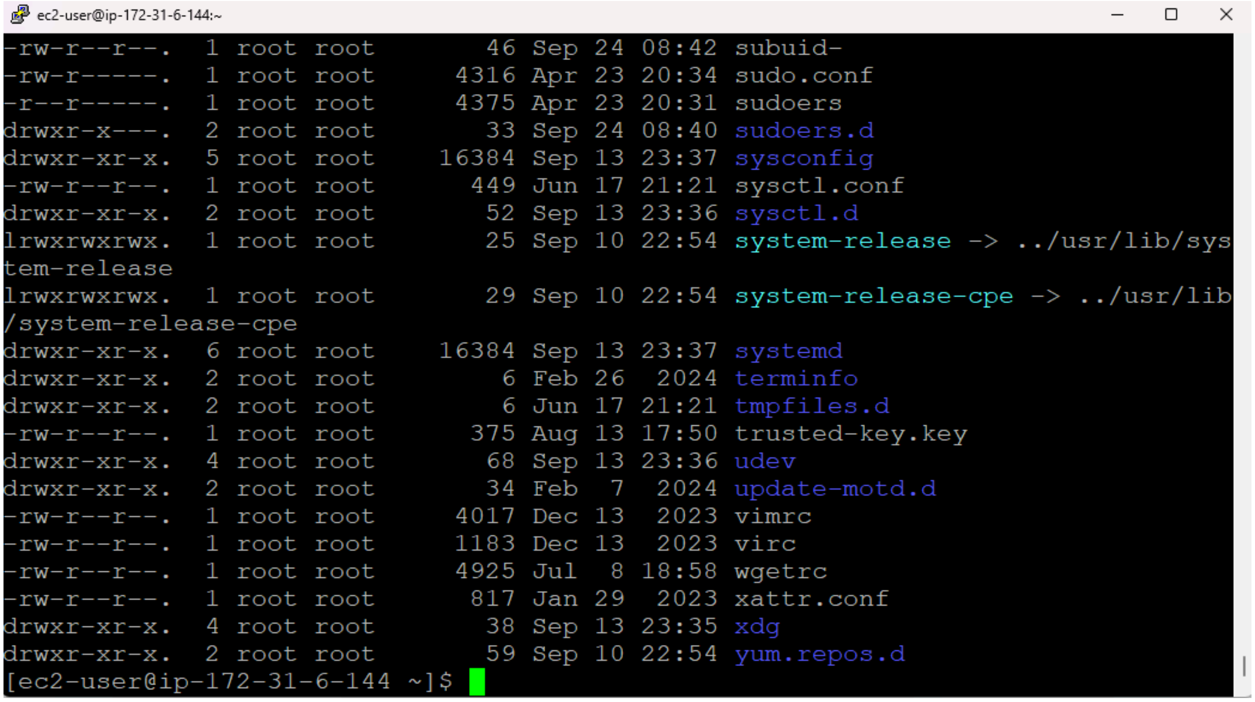
```
[    3.548948] fuse: init (API version 7.37)
[    3.620121] systemd-journald[1092]: Received client request to flush runtime
[    4.039574] input: Power Button as /devices/LNXSYSTM:00/LNXPWRBN:00/input/in
[    4.052015] i8042: PNP: PS/2 Controller [PNP0303:PS2K,PNP0f13:PS2M] at 0x60,
[    4.053788] i8042: Warning: Keylock active
[    4.084472] serio: i8042 KBD port at 0x60,0x64 irq 1
[    4.085710] serio: i8042 AUX port at 0x60,0x64 irq 12
[    4.087178] ACPI: button: Power Button [PWRF]
[    4.088346] input: Sleep Button as /devices/LNXSYSTM:00/LNXSLPBN:00/input/in
[    4.090359] vif vif-0 enX0: renamed from eth0
[    4.092366] ACPI: button: Sleep Button [SLPF]
[    4.234748] SCSI subsystem initialized
[    4.275368] libata version 3.00 loaded.
[    4.313831] ata_piix 0000:00:01.1: version 2.13
[    4.322609] scsi host0: ata_piix
[    4.332831] scsi host1: ata_piix
[    4.334365] ata1: PATA max MWDMA2 cmd 0x1f0 ctl 0x3f6 bmdma 0xc000 irq 14
[    4.335824] ata2: PATA max MWDMA2 cmd 0x170 ctl 0x376 bmdma 0xc008 irq 15
[    4.358783] zram_generator::config[1915]: zram0: system has too much memory
[    4.529121] RPC: Registered named UNIX socket transport module.
[    4.530471] RPC: Registered udp transport module.
[    4.531602] RPC: Registered tcp transport module.
[    4.532738] RPC: Registered tcp NFSv4.1 backchannel transport module.
[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 10 – Command (lspci)



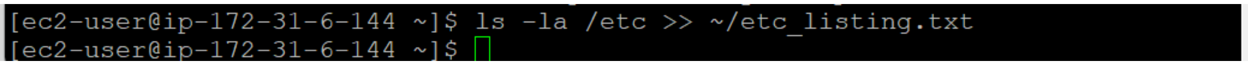
```
[ec2-user@ip-172-31-6-144 ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 11 – Command (ls -la /etc)



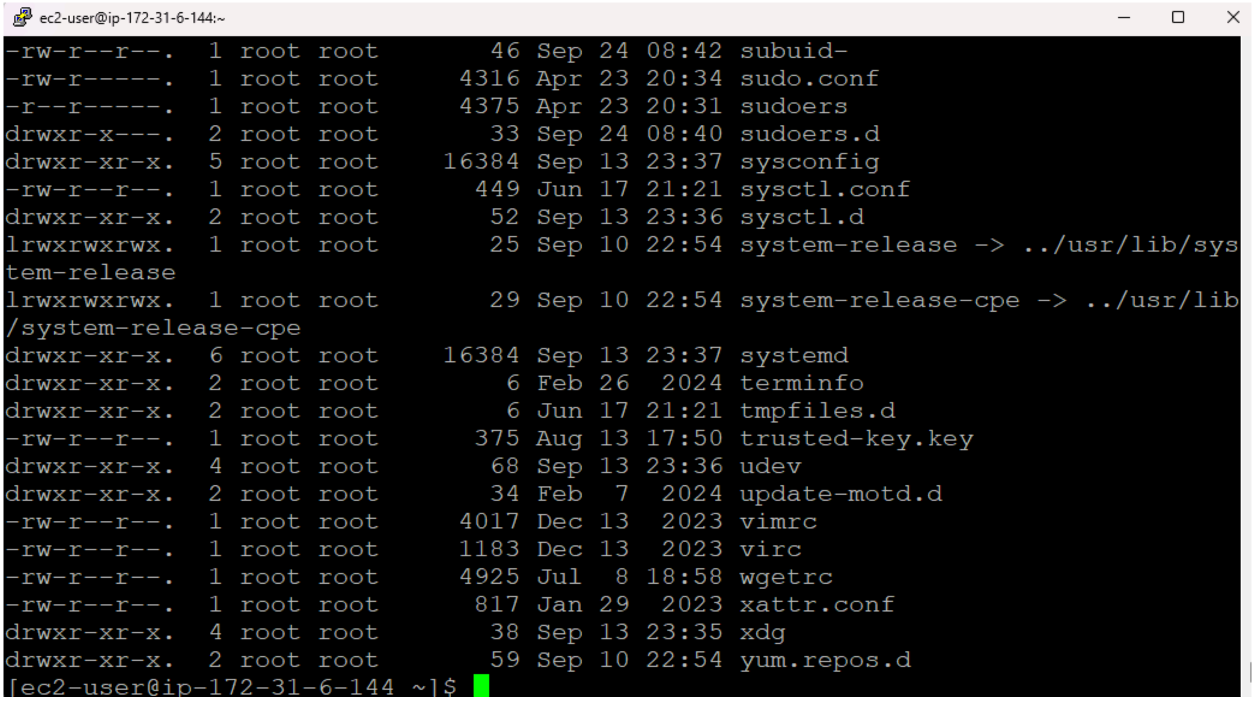
```
-rw-r--r--.  1 root root     46 Sep 24 08:42 subuid-
-rw-r-----.  1 root root   4316 Apr 23 20:34 sudo.conf
-r--r-----.  1 root root   4375 Apr 23 20:31 sudoers
drwxr-x---.  2 root root     33 Sep 24 08:40 sudoers.d
drwxr-xr-x.  5 root root  16384 Sep 13 23:37 sysconfig
-rw-r--r--.  1 root root    449 Jun 17 21:21 sysctl.conf
drwxr-xr-x.  2 root root     52 Sep 13 23:36 sysctl.d
lrwxrwxrwx.  1 root root     25 Sep 10 22:54 system-release -> ../usr/lib/sys
tem-release
lrwxrwxrwx.  1 root root     29 Sep 10 22:54 system-release-cpe -> ../usr/lib
/system-release-cpe
drwxr-xr-x.  6 root root  16384 Sep 13 23:37 systemd
drwxr-xr-x.  2 root root      6 Feb 26  2024 terminfo
drwxr-xr-x.  2 root root      6 Jun 17 21:21 tmpfiles.d
-rw-r--r--.  1 root root    375 Aug 13 17:50 trusted-key.key
drwxr-xr-x.  4 root root     68 Sep 13 23:36 udev
drwxr-xr-x.  2 root root     34 Feb  7  2024 update-motd.d
-rw-r--r--.  1 root root   4017 Dec 13  2023 vimrc
-rw-r--r--.  1 root root   1183 Dec 13  2023 virc
-rw-r--r--.  1 root root   4925 Jul  8 18:58 wgetrc
-rw-r--r--.  1 root root    817 Jan 29  2023 xattr.conf
drwxr-xr-x.  4 root root     38 Sep 13 23:35 xdg
drwxr-xr-x.  2 root root     59 Sep 10 22:54 yum.repos.d
[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 12 – Command (ls -la /etc >> ~/etc_listing.txt)



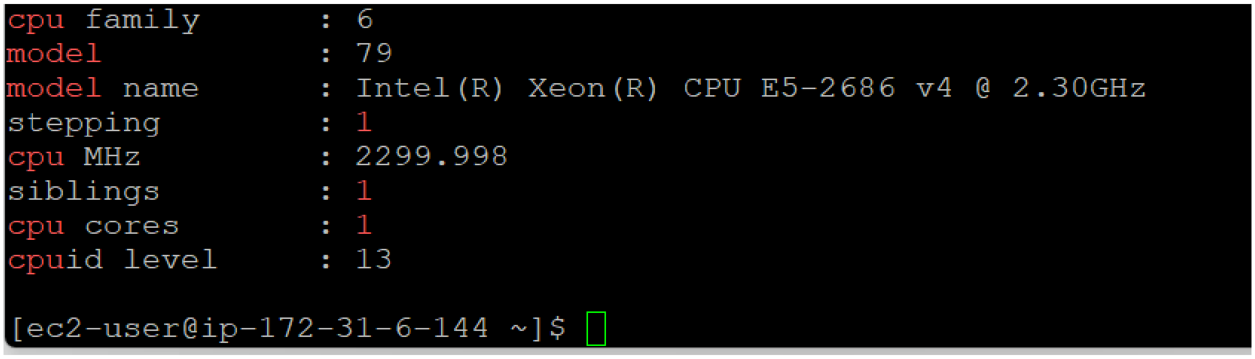
```
[ec2-user@ip-172-31-6-144 ~]$ ls -la /etc >> ~/etc_listing.txt
[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 13 – Command (cat ~/etc_listing.txt)



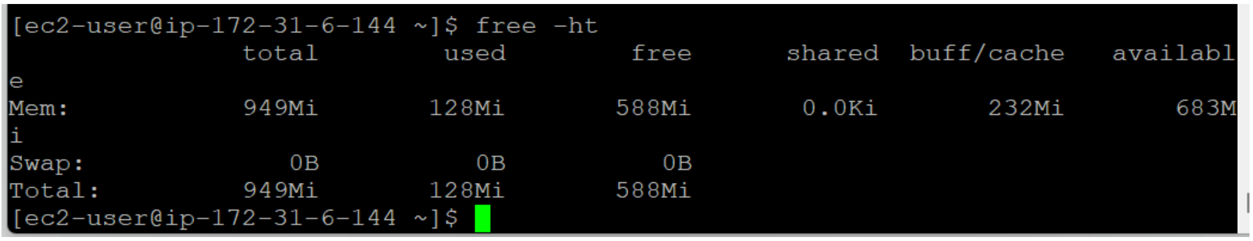
```
-rw-r--r--.  1 root root      46 Sep 24 08:42 subuid-
-rw-r-----.  1 root root    4316 Apr 23 20:34 sudo.conf
-r--r-----.  1 root root    4375 Apr 23 20:31 sudoers
drwxr-x---.  2 root root      33 Sep 24 08:40 sudoers.d
drwxr-xr-x.  5 root root   16384 Sep 13 23:37 sysconfig
-rw-r--r--.  1 root root     449 Jun 17 21:21 sysctl.conf
drwxr-xr-x.  2 root root      52 Sep 13 23:36 sysctl.d
lrwxrwxrwx.  1 root root      25 Sep 10 22:54 system-release -> ../usr/lib/sys
tem-release
lrwxrwxrwx.  1 root root      29 Sep 10 22:54 system-release-cpe -> ../usr/lib
/system-release-cpe
drwxr-xr-x.  6 root root   16384 Sep 13 23:37 systemd
drwxr-xr-x.  2 root root       6 Feb 26  2024 terminfo
drwxr-xr-x.  2 root root       6 Jun 17 21:21 tmpfiles.d
-rw-r--r--.  1 root root     375 Aug 13 17:50 trusted-key.key
drwxr-xr-x.  4 root root      68 Sep 13 23:36 udev
drwxr-xr-x.  2 root root      34 Feb  7  2024 update-motd.d
-rw-r--r--.  1 root root    4017 Dec 13  2023 vimrc
-rw-r--r--.  1 root root    1183 Dec 13  2023 virc
-rw-r--r--.  1 root root    4925 Jul  8 18:58 wgetrc
-rw-r--r--.  1 root root     817 Jan 29  2023 xattr.conf
drwxr-xr-x.  4 root root      38 Sep 13 23:35 xdg
drwxr-xr-x.  2 root root      59 Sep 10 22:54 yum.repos.d
[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 14 – Command (cat /proc/cpuinfo | grep -I -e ’^cpu’ -e ’1$’ -e ’^$’)



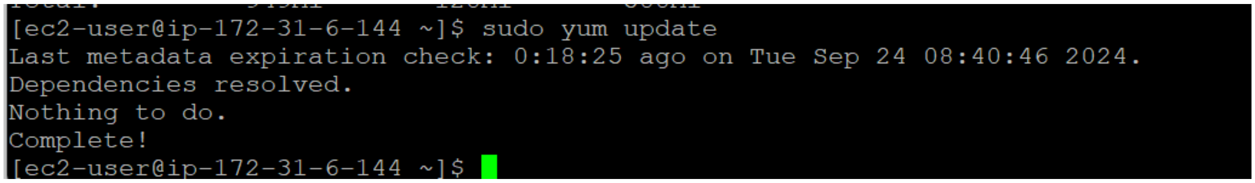
```
cpu family      : 6
model           : 79
model name      : Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
stepping        : 1
cpu MHz         : 2299.998
siblings        : 1
cpu cores       : 1
cpuid level     : 13

[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 15 – Command (free -ht)



```
[ec2-user@ip-172-31-6-144 ~]$ free -ht
               total        used        free      shared  buff/cache   availabl
e
Mem:           949Mi       128Mi       588Mi       0.0Ki       232Mi       683M
i
Swap:             0B          0B          0B
Total:         949Mi       128Mi       588Mi
[ec2-user@ip-172-31-6-144 ~]$
```

Screenshot 16 – Command (sudo yum update)



```
[ec2-user@ip-172-31-6-144 ~]$ sudo yum update
Last metadata expiration check: 0:18:25 ago on Tue Sep 24 08:40:46 2024.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-6-144 ~]$
```

From the data in the output from the above commands answer the following:

Question 6: From the data in the output from these commands:

A:

- *How many and what type of processors does your server have?*
    - ***1 Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz with1 cpu core***
- How much physical memory does your virtual machine have installed?
    - ***949 Mi***
- How much physical memory does your virtual machine have available?
    - ***683 Mi***
- What is the exact version number of the Linux kernel in use?
    - ***Linux version 6.1.109-118.189.amzn2023.x86_64 (mockbuild@ip-10-0-63-165) (gcc (GCC) 11.4.1 20230605 (Red Hat 11.4.1-2), GNU ld version 2.39-6.amzn2023.0.10) #1 SMP PREEMPT_DYNAMIC Tue Sep 10 08:59:12 UTC 2024***

***Deliverables for assignment 1 include this document completed. You will submit the document in canvas.