CSE 311 HW 2:

Exercise 1:

Part (a):

1. cd /usr/local/bin

   Changes the current working directory to /usr/local/bin.

2. rm -r ~/temp

   Recursively removes the directory ~/temp and all its contents.

3. cat input.txt > output.txt

   Redirects the contents of input.txt to output.txt, overwriting output.txt if it already exists.

4. echo "a random string" >> output.txt

   Appends the string "a random string" to the file output.txt.

5. cp output.txt ~/

   Copies the file output.txt to the user's home directory.

6. less output.txt | grep "str"

   Opens output.txt in less and filters its contents to show only lines that contain the substring "str".

7. ls -S | tail -1

   Lists files in the current directory sorted by size in descending order and displays the smallest file.

8. more output.txt | head -n 5 | tail -3 > ~/result.txt

   Displays the first 5 lines of output.txt, extracts the last 3 of those lines, and saves them to ~/result.txt.

9. scp -P 130 netid@sparky.ic.sunysb.edu:~/file .

   Securely copies file from the remote server sparky.ic.sunysb.edu (using port 130) to the current directory.

10. sudo cat /etc/sudoers

    Displays the contents of /etc/sudoers using cat, requiring superuser privileges.

Part (b):

1. Create a file called "myscript" and make it executable by everyone

   ```
   touch myscript
   chmod a+x myscript
   ```

2. Execute the script "myscript" and save the output to a file called "result.txt"

   ```
   ./myscript > result.txt
   ```

3. Move "result.txt" to the parent directory (one level above the current directory)

   ```
   mv result.txt ../
   ```

4. Count the total number of files in the current directory, including hidden files

   ```
   ls -A | wc -l
   ```

5. Download the webpage "www.cs.stonybrook.edu" and save it in your home directory

   ```
   wget -O ~/index.html www.cs.stonybrook.edu
   ```

6. Search for and display all files named "myfile" in your home directory

   ```
   find ~/ -type f -name "myfile"
   ```

7. Show all lines in the file "testfile" that contain the word "test" (case-insensitive)

   ```
   grep -i "test" testfile
   ```

8. Stop the process with the ID 13572, which is in a zombie state

   ```
   kill -9 13572
   ```

9. Create a directory called "temp" in the root directory

   ```
   sudo mkdir /temp
   ```

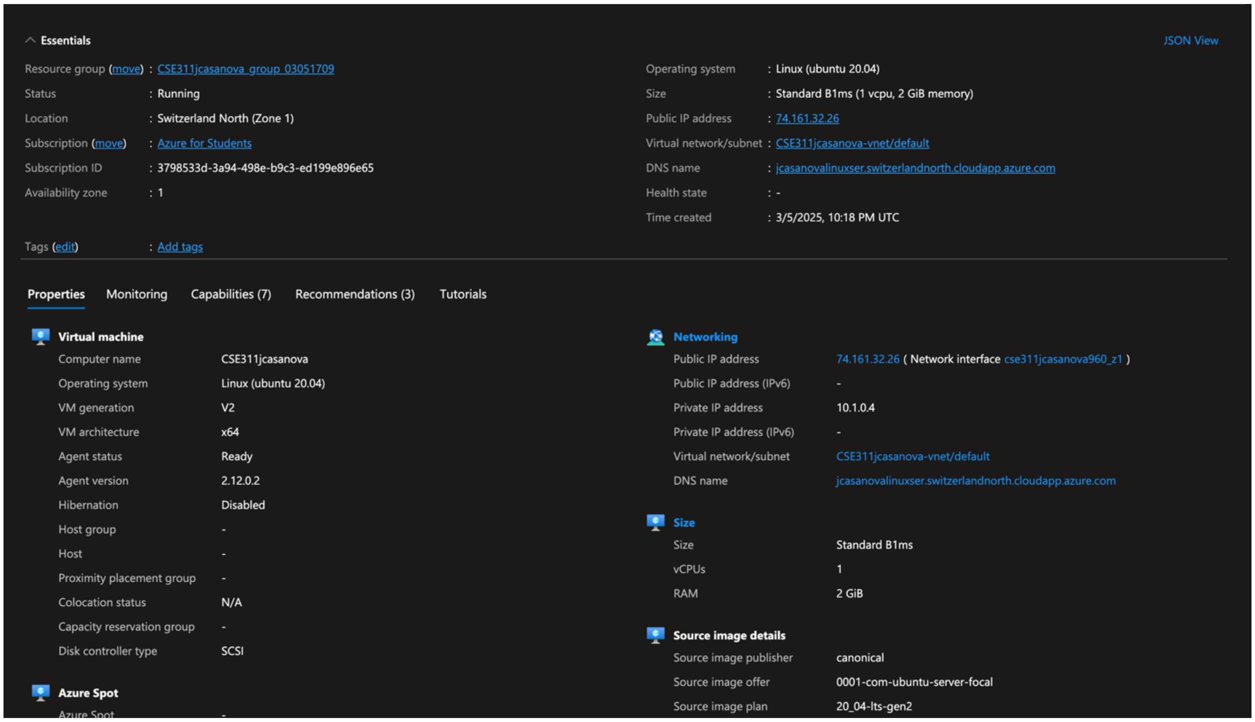
10. After creating "temp", add two files (fileA and fileB), and then delete the directory "temp" and its contents

    ```
    sudo touch /temp/fileA /temp/fileB
    sudo rm -r /temp
    ```

Exercise 2:

VM info: Using the Azure VM

IP: 74.161.32.26



Resource group (move)	: CSE311jcasanova_group_03051709
Status	: Running
Location	: Switzerland North (Zone 1)
Subscription (move)	: Azure for Students
Subscription ID	: 3798533d-3a94-498e-b9c3-ed199e896e65
Availability zone	: 1
Tags (edit)	: Add tags

Operating system	: Linux (ubuntu 20.04)
Size	: Standard B1ms (1 vcpu, 2 GiB memory)
Public IP address	: 74.161.32.26
Virtual network/subnet	: CSE311jcasanova-vnet/default
DNS name	: jcasanovalinuxser.switzerlandnorth.cloudapp.azure.com
Health state	: -
Time created	: 3/5/2025, 10:18 PM UTC

Virtual machine

Computer name	CSE311jcasanova
Operating system	Linux (ubuntu 20.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.12.0.2
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Azure Spot

Azure Spot	-

Networking

Public IP address	74.161.32.26 (Network interface cse311jcasanova960_z1)
Public IP address (IPv6)	-
Private IP address	10.1.0.4
Private IP address (IPv6)	-
Virtual network/subnet	CSE311jcasanova-vnet/default
DNS name	jcasanovalinuxser.switzerlandnorth.cloudapp.azure.com

Size

Size	Standard B1ms
vCPUs	1
RAM	2 GiB

Source image details

Source image publisher	canonical
Source image offer	0001-com-ubuntu-server-focal
Source image plan	20_04-lts-gen2

Making TA account

Password will be Ta@cse311

Adding the ta user

sudo adduser ta

then I switch into the ta user and then made the directory and also gave it the right permissions

sudo su - ta

mkdir -p ~/.ssh

chmod 700 ~/.ssh

added the key give in the doc

nano ~/.ssh/authorized_keys

then set permissions

chmod 600 ~/.ssh/authorized_keys

then exit the ta user with

```
exit
```

Protecting Your System with Fail2ban

```
sudo apt update

sudo apt install fail2ban

sudo systemctl enable fail2ban

sudo systemctl start fail2ban

sudo nano /etc/fail2ban/jail.local
```

Pasted this into jail.local:

```
[sshd]

enabled = true

banaction = iptables-multiport

maxretry = 5

findtime = 15m

bantime = 25m
```

given the parameters in the doc

restarted it

```
sudo systemctl restart fail2ban
```

Then to check if it was working

```
sudo systemctl status fail2ban
```

Configuring Administrative Access

Exercise 3:

To open /etc/sudoers

```
sudo visudo
```

Went all the way to the bottom to add this line

```
ta ALL=(ALL) NOPASSWD:ALL
```

Saved it and then went to test it out

```
sudo su ta
```

```
sudo touch /etc/ta-write-successful
```

Used

```
ls -l /etc/ta-write-successful
```

to check if it works which it did

didn’t delete the file

Time Synchronization (NTP)

```
sudo apt update
```

Installed NTP

```
sudo apt install ntp
```

Checked the ntp.conf file to make sure everything was good

```
sudo nano /etc/ntp.conf
```

restarted it

```
sudo systemctl restart ntp
```

enable it

```
sudo systemctl enable ntp
```

Made sure it was active

```
sudo systemctl status ntp
```

Disabling Root Login

Opened up sshd_config

```
sudo nano /etc/ssh/sshd_config
```

Then looked for the PermitRootLogin and changed it to no

Saved the file and then restarted it

```
sudo systemctl restart sshd
```