SERVER AZURE PROJECT ON SECURITY IPTABLES ANALYSIS

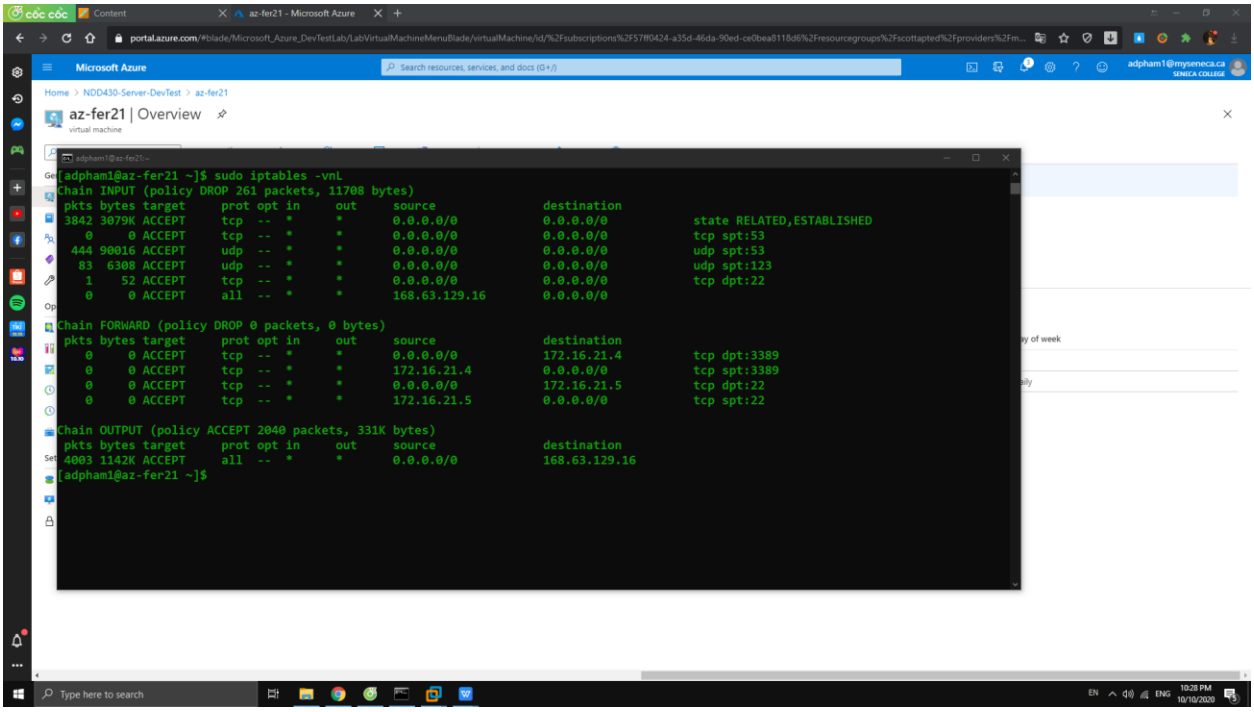
Windows Server Pre-deployment Configurations

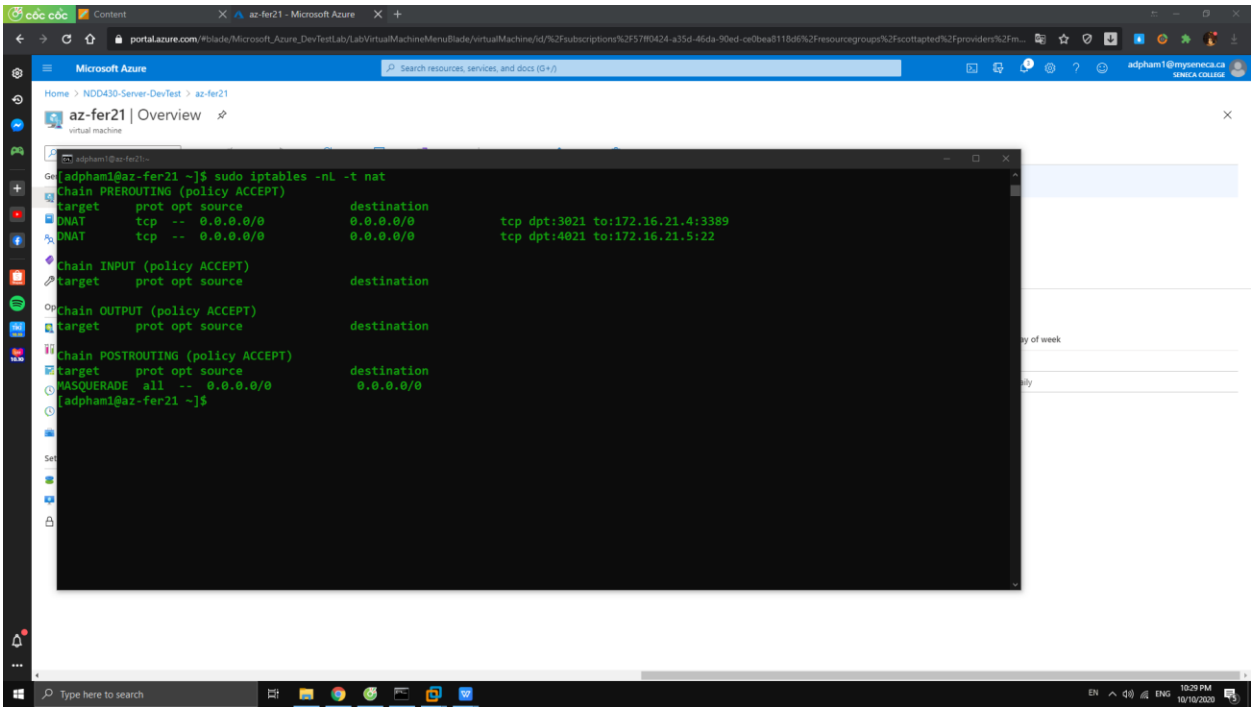
Analyze the iptables script **iptables-start** and **<u>understand what it does</u>**. You will need to modify it slightly to make it work with your network.

Change the RDP access port to 30XX **(XX is your unique ID number)**

Edit IP addresses if necessary

Copy the iptables script to your **az-ferXX** VM. Log in and run the script. **Do not save the configuration at this time.**





Log out and confirm you can log back in to the **az-ferXX** VM.

1) Flush everything

sudo iptables -F

sudo iptables -X

sudo iptables -t nat -F

sudo iptables -t nat -X

2) RDP and SSH iptables

sudo iptables -t nat -A PREROUTING -p tcp --dport 3021 -j DNAT --to-destination 172.16.21.4:3389

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

3) Allow traffic through dport and sport

sudo iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A INPUT -p tcp --sport 53 -j ACCEPT

sudo iptables -A INPUT -p udp --sport 53 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -p udp --sport 123 -j ACCEPT

sudo iptables -A INPUT -s 168.63.129.16 -j ACCEPT

sudo iptables -A OUTPUT -d 168.63.129.16 -j ACCEPT

sudo iptables -A FORWARD -p tcp -s 172.16.21.4 --sport 3389 -j ACCEPT

sudo iptables -A FORWARD -p tcp -d 172.16.21.4 --dport 3389 -j ACCEPT

4) Drop INPUT, FORWARD and save iptables

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

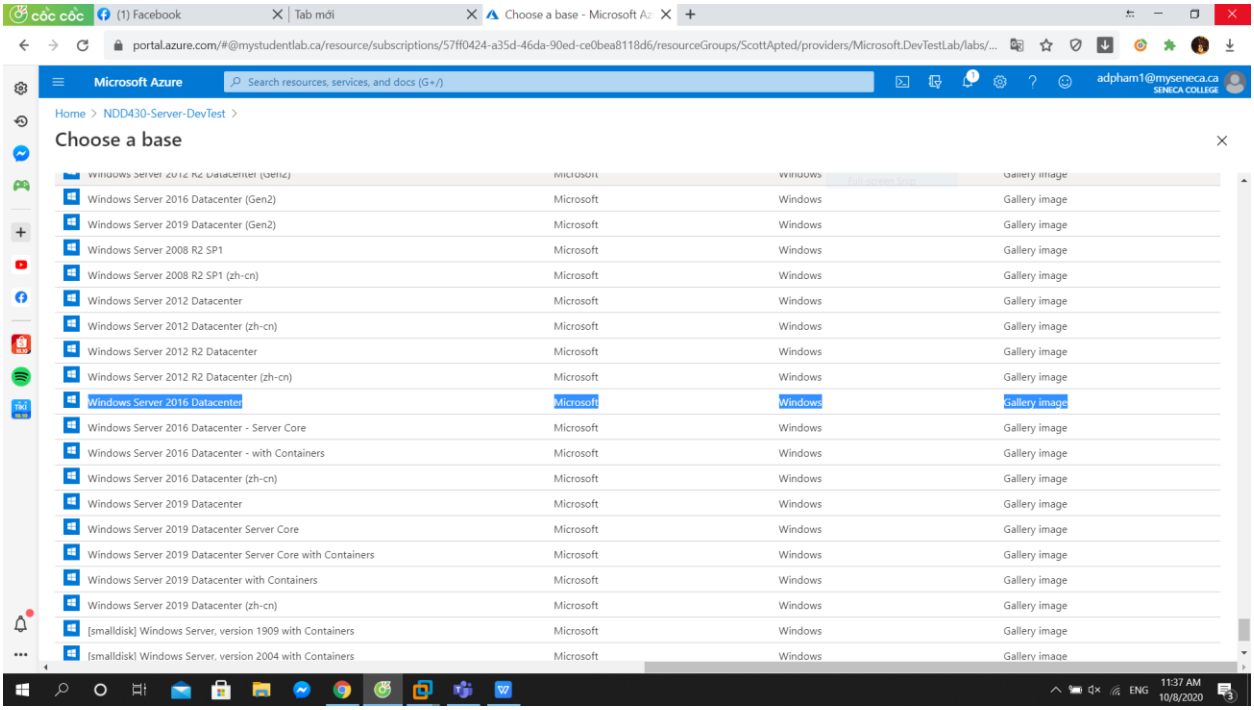
sudo service iptables save

Install and configure Azure Windows Server

Log into the Azure Portal and access the **NDD430-Server-DevTest** Lab via the link provided to you in Teams.

Add a virtual machine with the following specifications:

When asked to choose a base Select the **Windows Server 2016 Datacenter** image **(NOT GEN 2)**



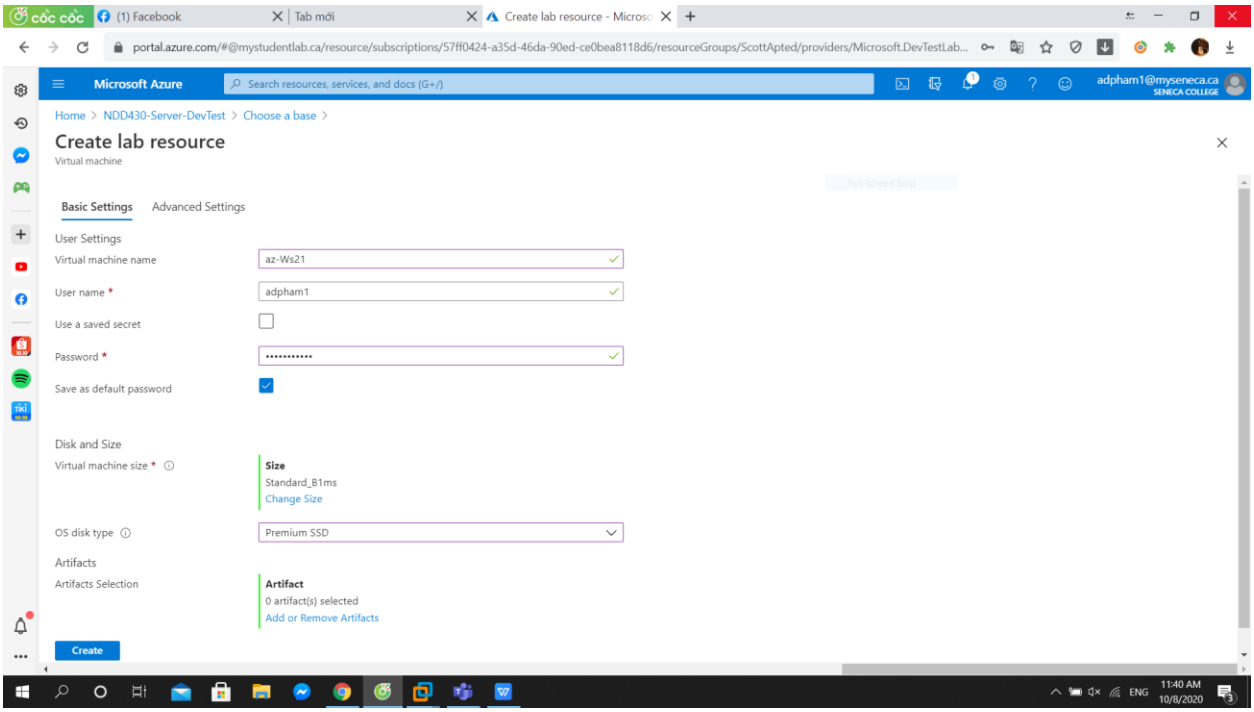
Basic Settings:

VM name = **az-Ws#XX (replace #XX with the unique identifier assigned to you i.e. az-ws85)**

Create a Username and password. **Note: Please read the following about [creating good passwords and good password management.]**

Select **B2ms** for VM size

Select **Premium SSD**



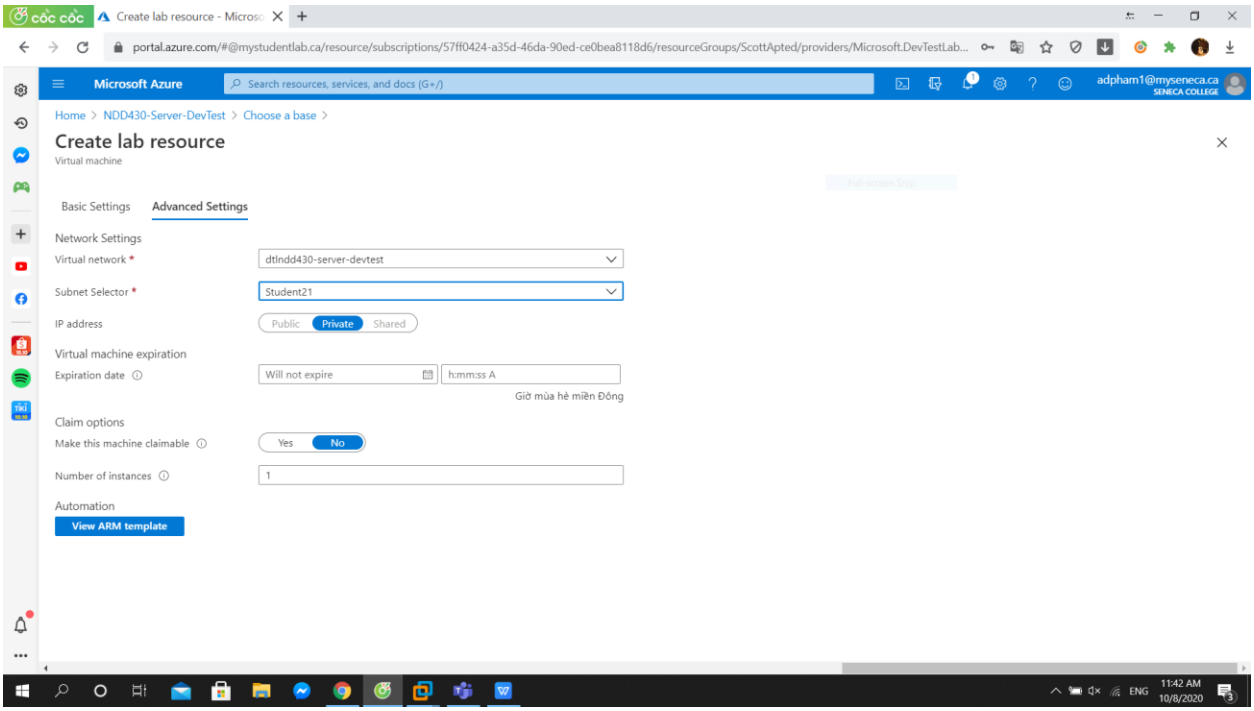
Advanced settings:

Network = dtlndd430-server-devtest

Subnet = **StudentXX (Find the subnet in the list with your unique ID)**

Choose **Private IP**

Press Create to deploy the VM



Post deployment configurations

Verify that you can RDP into your Windows server from your host **(What port should you use?)**

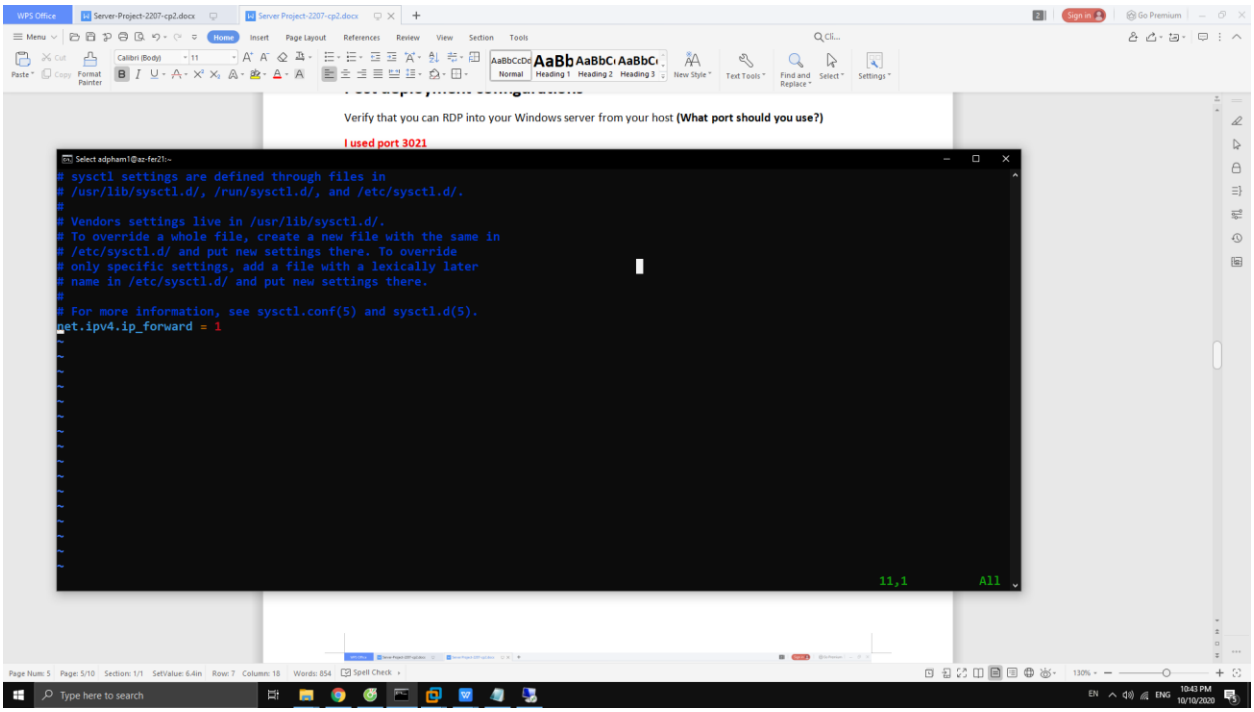
I used port 3021

Install the **Firefox** Web Browser

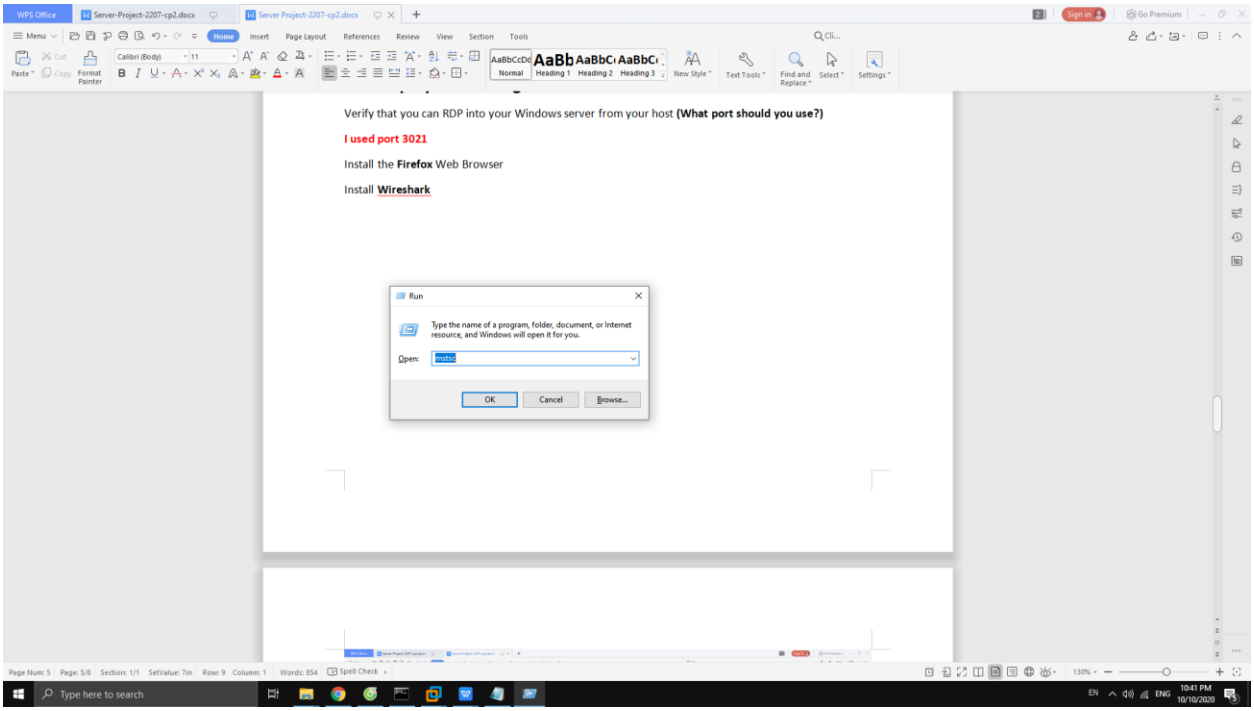
Install **Wireshark**

On az-fer21 issues this command to allow Remote desktop to az-Ws21

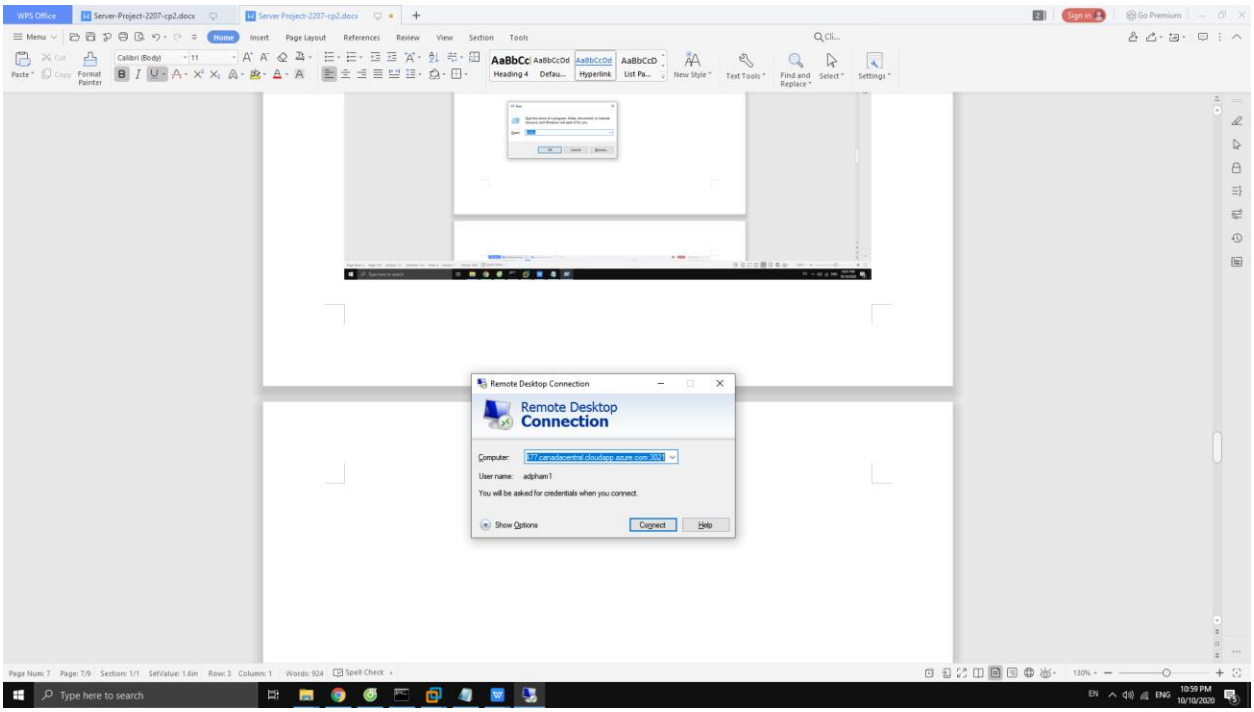
sudo vim /etc/sysctl.conf

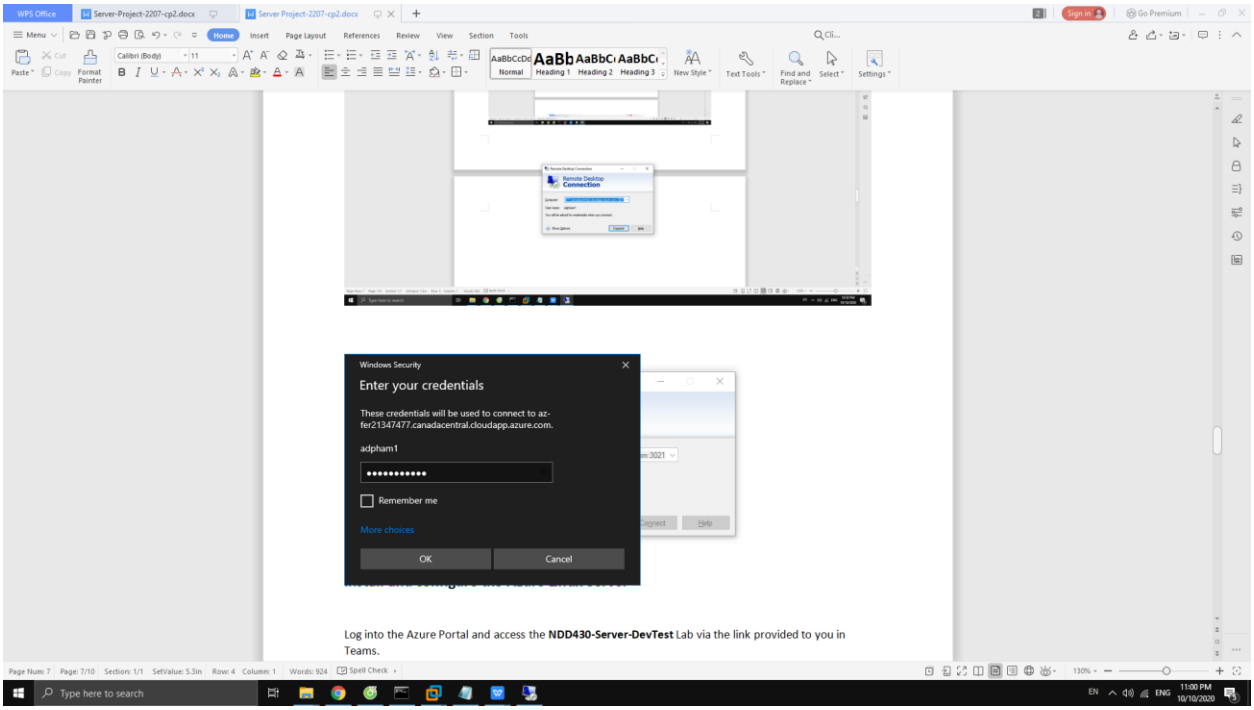


Then on your host desktop (PC,Laptop), open Run and issue mstsc to open remote desktop

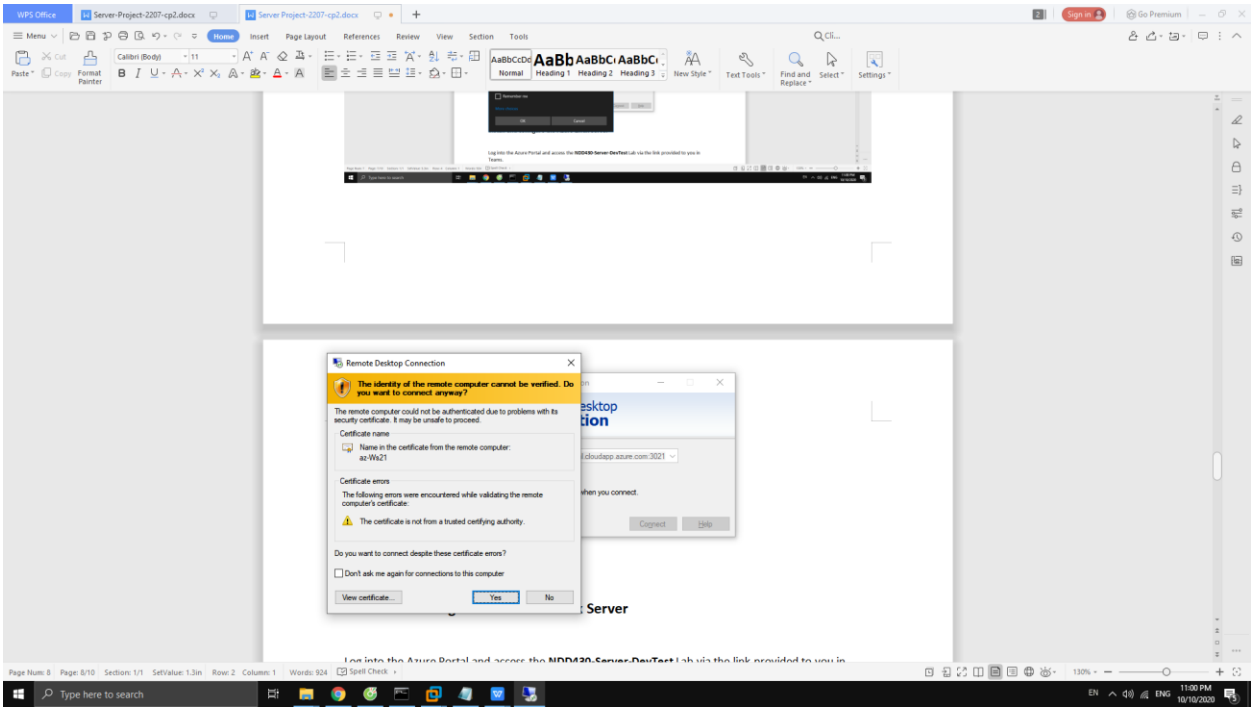


Copy the azure IP address or FQDN and add :3021 at the end then enter the password you generated before when installed az-Ws21 on azure.

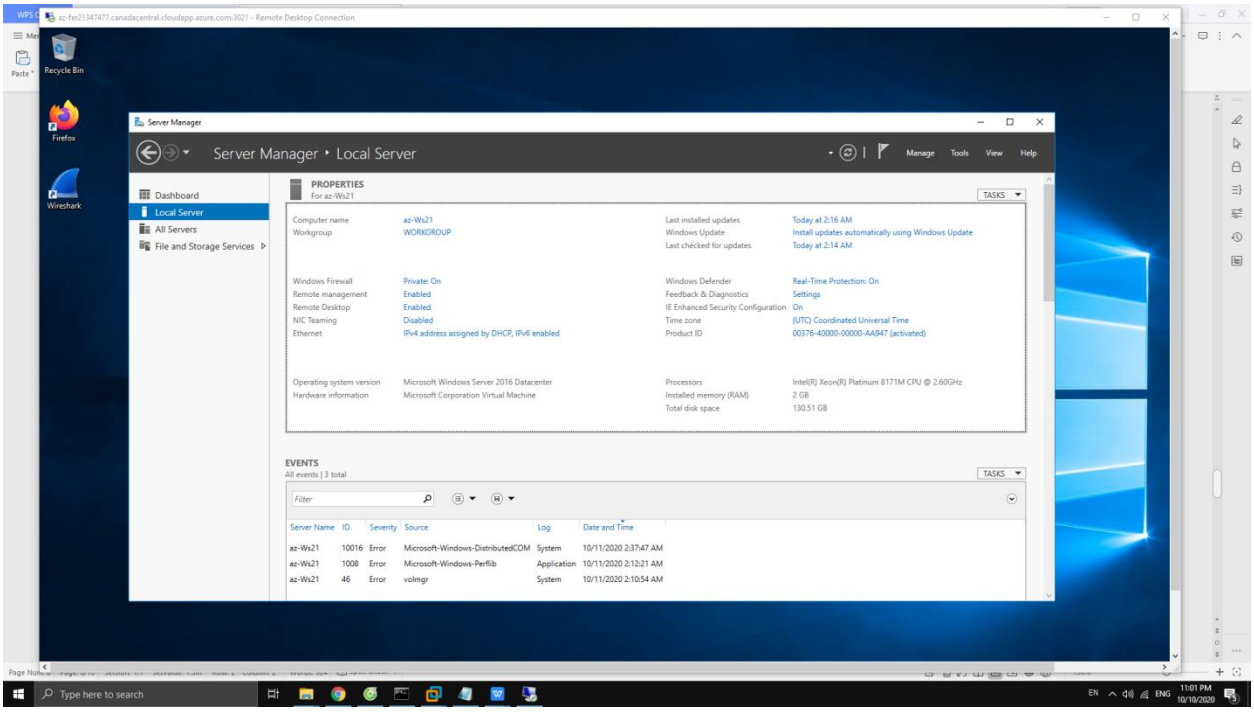




Then click yes to access to az-Ws21 via az-fer21 on your desktop



Then Install Wireshark and Firefox



Install and configure the Azure Linux Server

Log into the Azure Portal and access the **NDD430-Server-DevTest** Lab via the link provided to you in Teams.

Add a virtual machine with the following specifications:

When asked to choose a base Select the Rogue wave 7.7 **(choose the standard image, not the HPA image)**

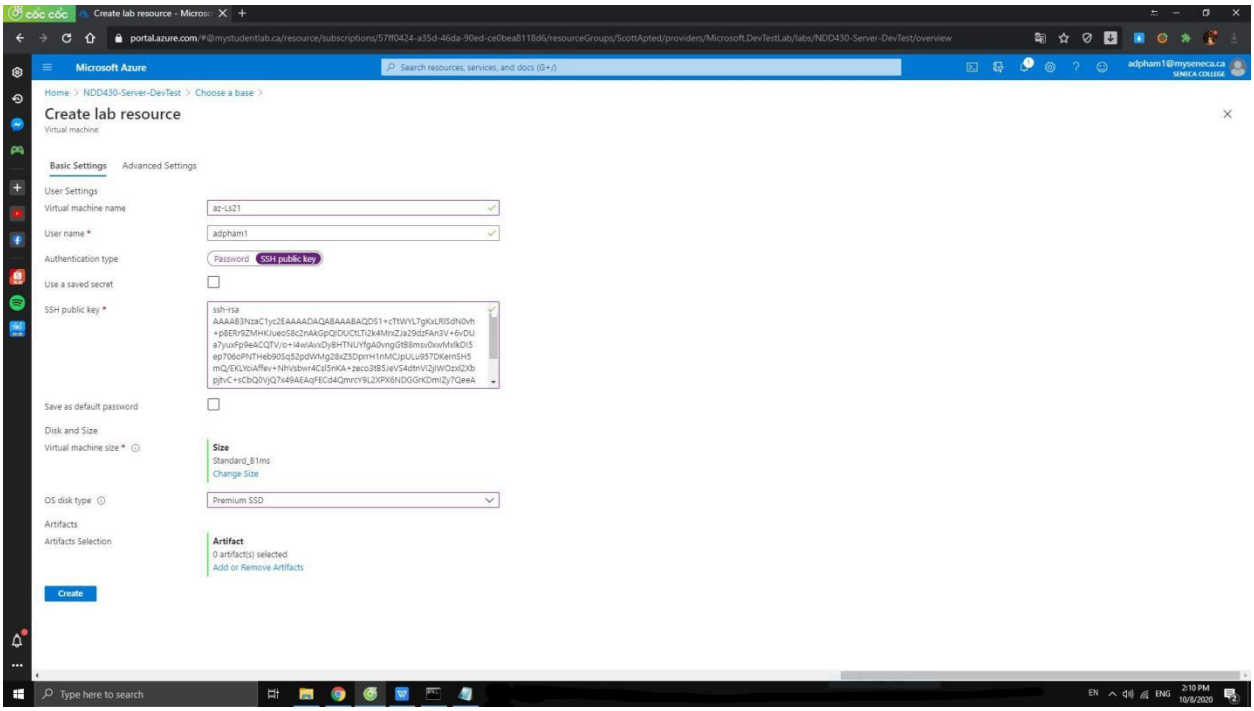
Basic Settings:

VM name = **az-Ls#XX (replace #XX with the unique identifier assigned to you i.e. az-Ls85)**

Set up an SSH key-pair to login from your Host machine **(use the same key that you used for the az-ferXX VM)**

Select **B1ms** for VM size

Select **Premium SSD**



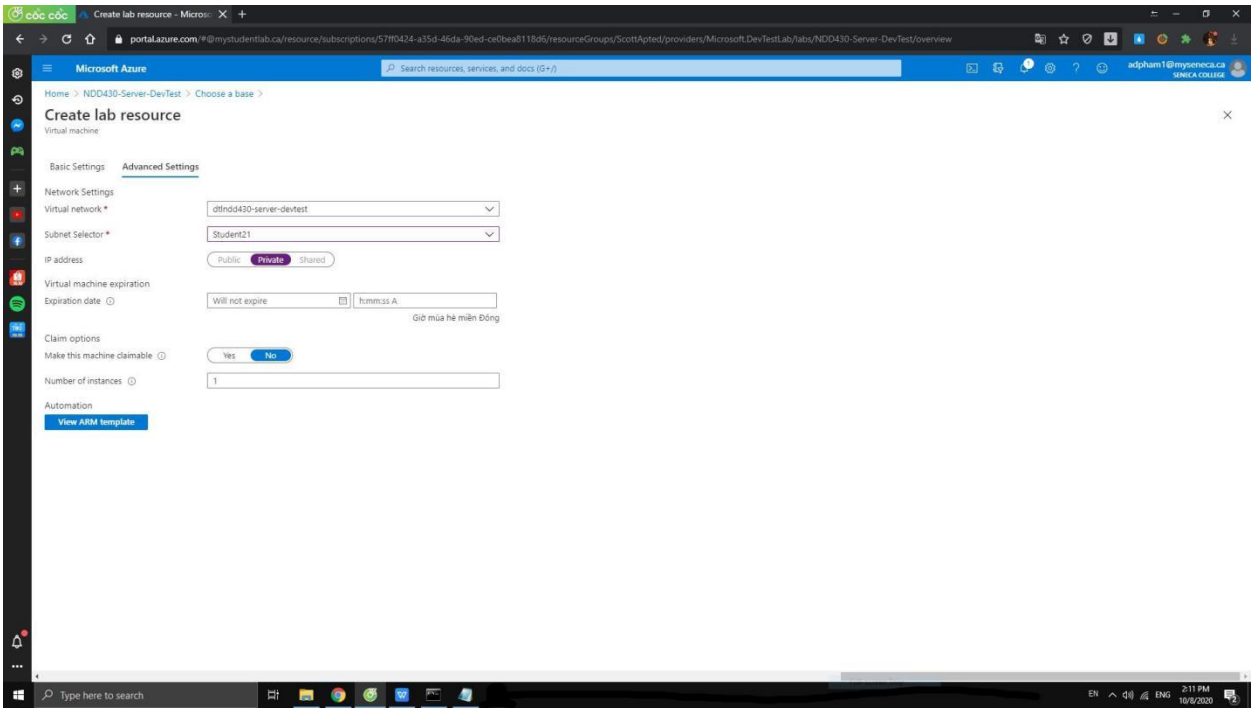
Advanced settings:

Network = dtlndd430-server-devtest

Subnet = **StudentXX (Find the subnet in the list with your unique ID)**

Choose **Private IP**

Press Create to deploy the VM



Post creation configurations

Edit the iptables file on your **az-ferXX** VM to allow SSH connections on port **40XX** to be redirected to port 22 on your **az-Ls** VM. Verify that you can log in to **az-LSXX** from your Host machine.

sudo iptables -t nat -A PREROUTING -p tcp --dport 4021 -j DNAT --to-destination 172.16.21.5:22

sudo iptables -A FORWARD -p tcp -d 172.16.21.5 --dport 22 -j ACCEPT

sudo iptables -A FORWARD -p tcp -s 172.16.21.5 --sport 22 -j ACCEPT

sudo service iptables save

port 22 on your az-Ls VM. Verify that you can log in to az-LSXX from your Host machine.

sudo iptables -t nat -A PREROUTING -p tcp –dport 4021 -j DNAT –to-destination 172.16.21.5:22

```
[adpham1@az-fer21 ~]$ sudo iptables -vnL
Chain INPUT (policy DROP 1351 packets, 69991 bytes)
 pkts bytes target     prot opt in     out     source               destination
20700   17M ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
 2394  489K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
  134 10184 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:123
   12   544 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     all  --  *      *       168.63.129.16        0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 9336 1009K ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.21.4         tcp dpt:3389
 6817 4678K ACCEPT     tcp  --  *      *       172.16.21.4          0.0.0.0/0           tcp spt:3389
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.21.5         tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       172.16.21.5          0.0.0.0/0           tcp spt:22

Chain OUTPUT (policy ACCEPT 10585 packets, 1782K bytes)
 pkts bytes target     prot opt in     out     source               destination
22556 6423K ACCEPT     all  --  *      *       0.0.0.0/0            168.63.129.16
[adpham1@az-fer21 ~]$
```

Perform the following actions on the az-LsXX VM:

```
[adpham1@az-fer21 ~]$ sudo iptables -nL -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:3021 to:172.16.21.4:3389
DNAT       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:4021 to:172.16.21.5:22

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0
[adpham1@az-fer21 ~]$
```

Perform the following actions on the az-LsXX VM:

Yum update

sudo yum update -y

Perform the following actions on the az-LsXX VM:

Yum update

sudo yum update -y

Yum autoremove firewalld

sudo yum autoremove firewalld

Yum install iptables-services

sudo yum install iptables-services -y

Enable iptables

sudo systemctl enable iptables

Start iptables

sudo systemctl start iptables

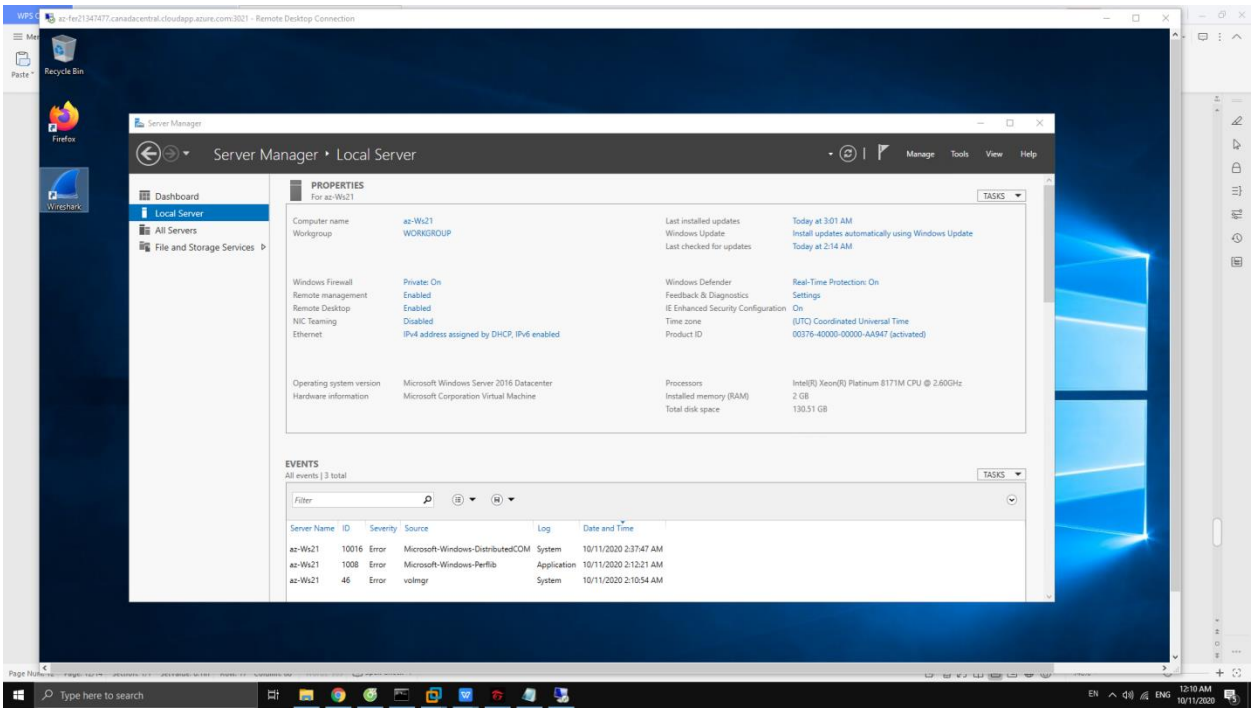
Additional Configurations Required

Install TCPDUMP on **ALL** CentOS machines in the project

Issue this command on CenOS machine

sudo yum install tcpdump -y

Install Wireshark on **ALL** Windows and Ubuntu Machines in the project

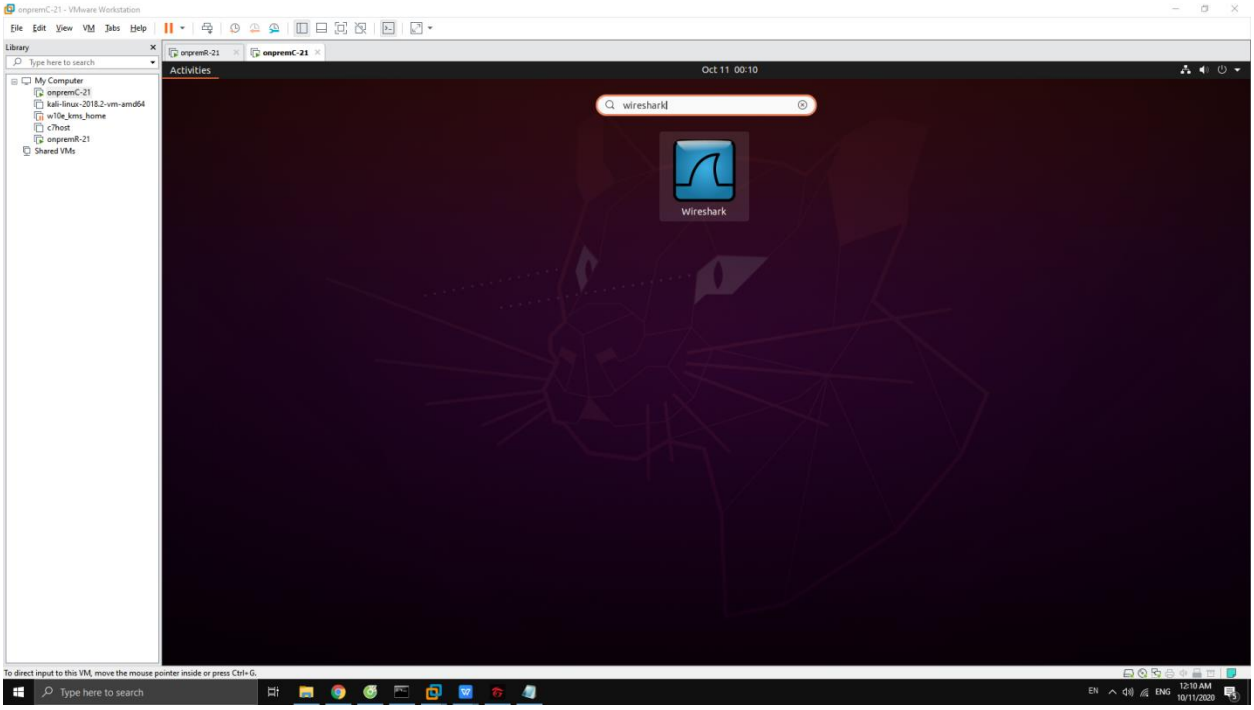


sudo apt install wireshark

Then click Yes to allow the installation

sudo usermod -aG wireshark $(whoami)

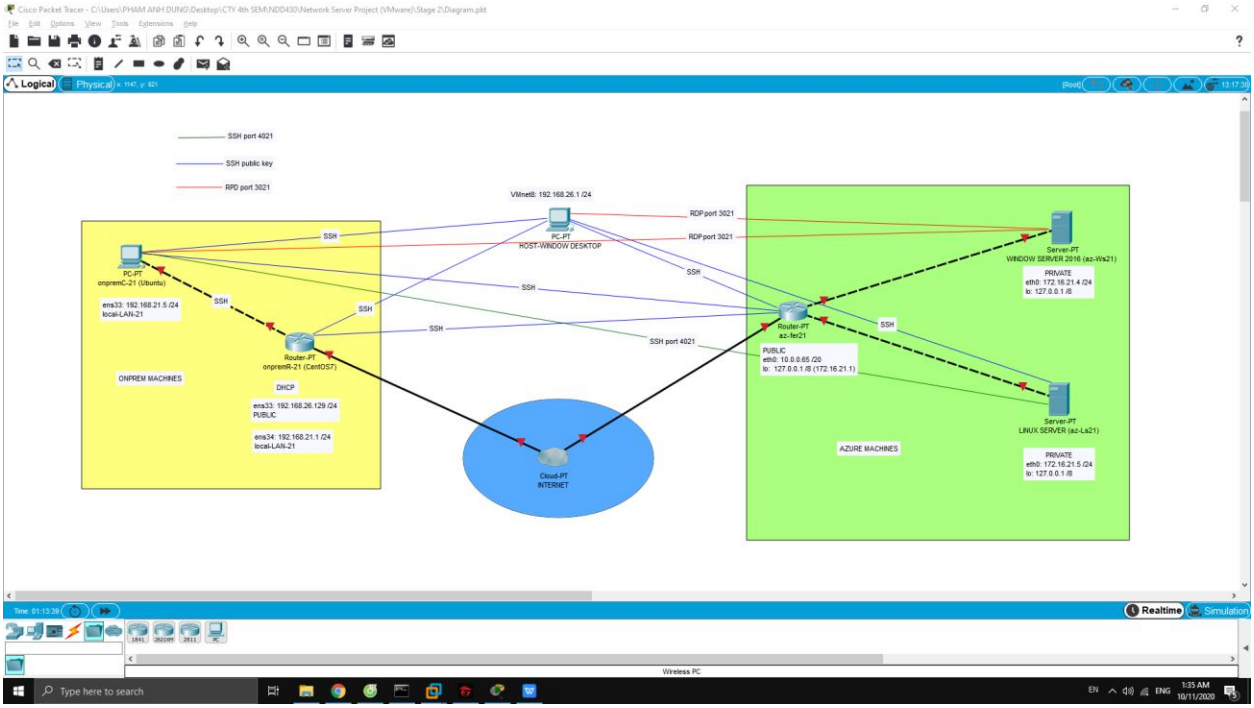
sudo reboot



Submit the following to Blackboard for documentation:

- Create a diagram of your network that shows the following information:

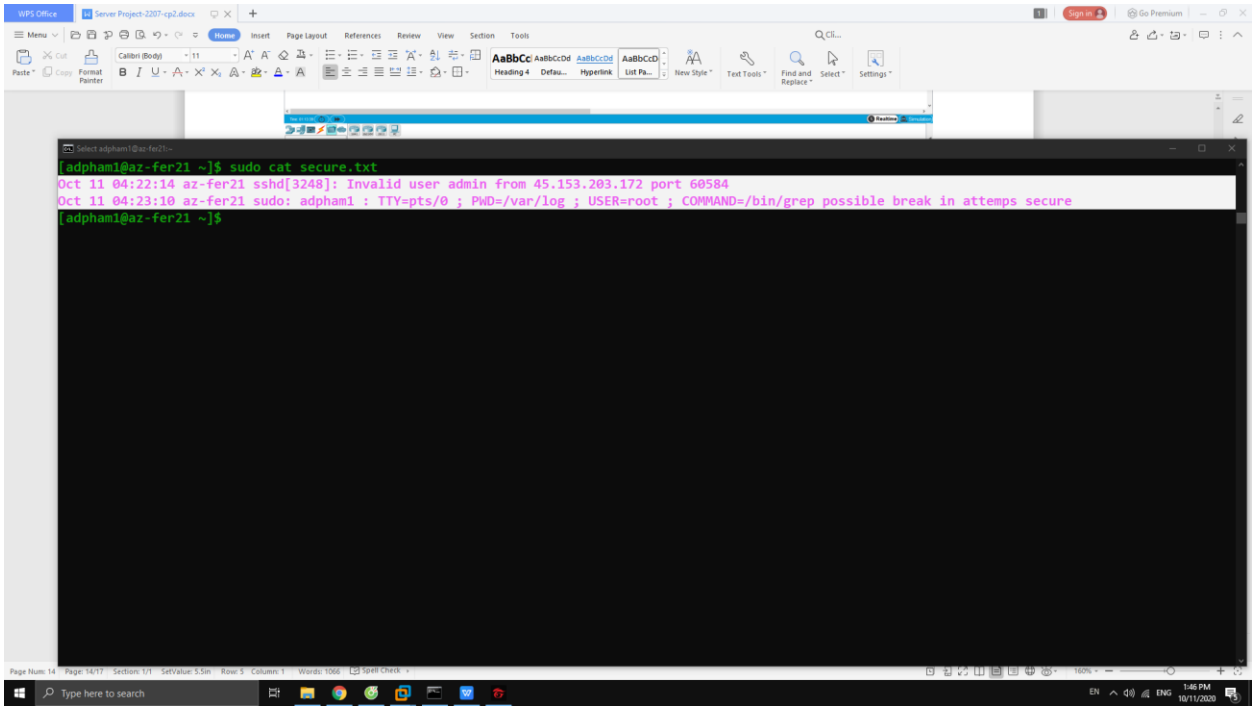
The topology – how all of the machines connect together including IP addresses, LAN segment information and locations of ssh keys.



- Examine all **secure** logs in **/var/log/** on the **az-ferXX** device. Create a new file that contains only "possible break in attempts" and "Invalid user" entries. **(Hint: is *grep* of any use here?)**

sudo cat /var/log/secure | grep "Invalid user" | head -1 > /home/adpham1/secure.txt

sudo cat /var/log/secure | grep "possible break in attemps" | head -1 >> /home/adpham1/secure.txt



- **Do the following steps:**

1. Execute the following command on your **onpremR** device:

   tcpdump -i any -qns0 > /home/***user***/packetlog.txt

2. ssh into your **az-LsXX** device from your **onpremC** device
3. Stop the **tcpdump** capture on your **onpremR** device
4. Search through the packetlog.txt file and create a new file that has only two packets – one with a source address of your client with TCP port **40XX** and one with a destination address of your client with TCP port **40XX**

sudo tcpdump -i any -qnns0 > /home/adpham1/packetlog.txt

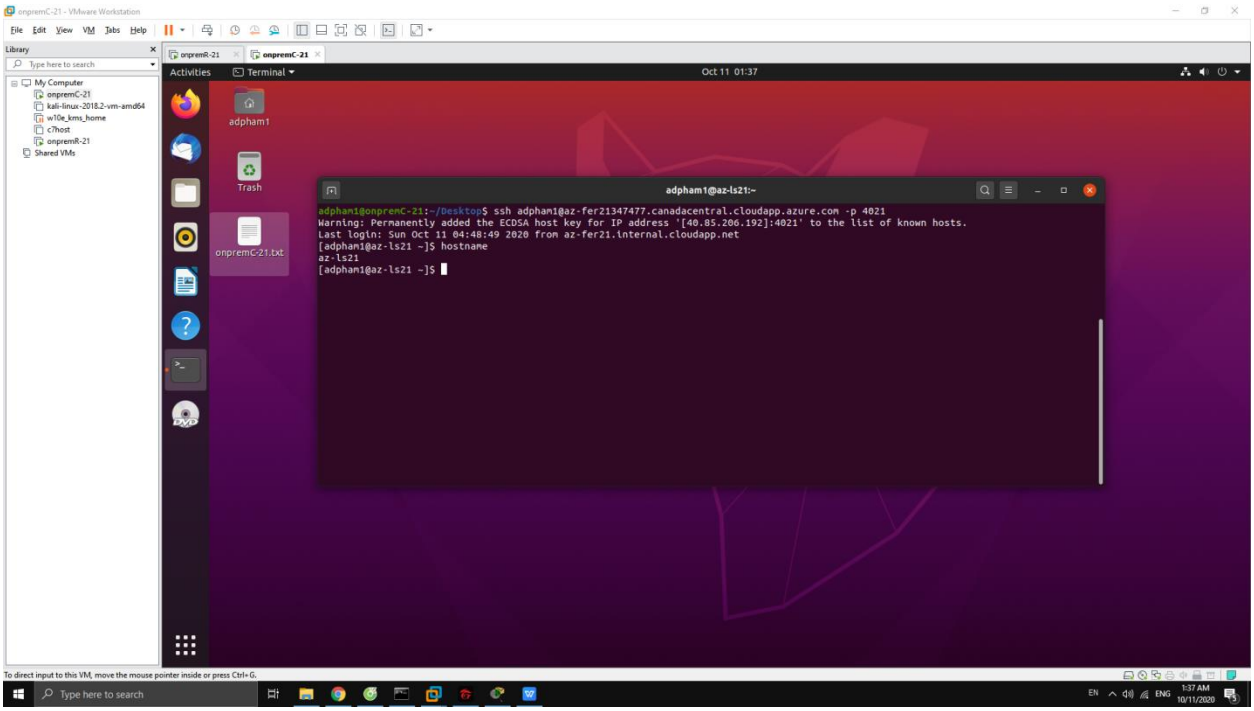
sudo cat packetlog.txt | grep "4021.*tcp" | head -3 | tail -2 > /home/adpham1/packetlog-new.txt

```
[adpham1@onpremR-21 ~]$ sudo cat packetlog.txt
11:35:21.099690 IP 192.168.26.129.68 > 192.168.26.254.67: UDP, length 300
11:35:21.099883 IP 192.168.26.254.67 > 192.168.26.129.68: UDP, length 300
11:35:23.342705 IP 192.168.21.5.68 > 192.168.21.1.67: UDP, length 288
11:35:23.343697 IP 192.168.21.1.67 > 192.168.21.5.68: UDP, length 300
11:35:24.366964 IP 192.168.21.5.35664 > 35.224.99.156.80: tcp 0
11:35:24.367013 IP 192.168.26.129.35664 > 35.224.99.156.80: tcp 0
11:35:24.391087 IP 35.224.99.156.80 > 192.168.26.129.35664: tcp 0
11:35:24.391096 IP 35.224.99.156.80 > 192.168.21.5.35664: tcp 0
11:35:24.391270 IP 192.168.21.5.35664 > 35.224.99.156.80: tcp 0
11:35:24.391300 IP 192.168.26.129.35664 > 35.224.99.156.80: tcp 0
11:35:24.391331 IP 192.168.21.5.35664 > 35.224.99.156.80: tcp 87
11:35:24.391335 IP 192.168.26.129.35664 > 35.224.99.156.80: tcp 87
11:35:24.391414 IP 35.224.99.156.80 > 192.168.26.129.35664: tcp 0
11:35:24.391420 IP 35.224.99.156.80 > 192.168.21.5.35664: tcp 0
11:35:24.415738 IP 35.224.99.156.80 > 192.168.26.129.35664: tcp 148
11:35:24.415744 IP 35.224.99.156.80 > 192.168.21.5.35664: tcp 148
11:35:24.415916 IP 192.168.21.5.35664 > 35.224.99.156.80: tcp 0
11:35:24.415923 IP 192.168.26.129.35664 > 35.224.99.156.80: tcp 0
11:35:24.415995 IP 35.224.99.156.80 > 192.168.26.129.35664: tcp 0
11:35:24.416002 IP 35.224.99.156.80 > 192.168.21.5.35664: tcp 0
11:35:24.752976 IP 192.168.21.5.48967 > 8.8.8.8.53: UDP, length 76
11:35:24.753018 IP 192.168.26.129.48967 > 8.8.8.8.53: UDP, length 76
11:35:24.753052 IP 192.168.21.5.47959 > 8.8.8.8.53: UDP, length 76
11:35:24.753057 IP 192.168.26.129.47959 > 8.8.8.8.53: UDP, length 76
11:35:24.764182 IP 8.8.8.8.53 > 192.168.26.129.47959: UDP, length 152
11:35:24.764209 IP 8.8.8.8.53 > 192.168.21.5.47959: UDP, length 152
11:35:24.796074 IP 8.8.8.8.53 > 192.168.26.129.48967: UDP, length 92
11:35:24.796100 IP 8.8.8.8.53 > 192.168.21.5.48967: UDP, length 92
11:35:24.796532 IP 192.168.21.5.58976 > 52.228.29.189.4021: tcp 0
```

```
[adpham1@onpremR-21 ~]$ sudo cat packetlog.txt | grep "4021.*tcp" | head -3 | tail -2 > /home/adpham1/packetlog-new.txt
[adpham1@onpremR-21 ~]$ sudo cat packetlog-new.txt
11:35:24.796554 IP 192.168.26.129.58976 > 52.228.29.189.4021: tcp 0
11:35:24.802475 IP 52.228.29.189.4021 > 192.168.26.129.58976: tcp 0
[adpham1@onpremR-21 ~]$
```

Checkpoint Demonstration

SSH from your **onpremC** to your **az-LsXX** machine



RDP from your **onpremC** to your **az-WsXX** machine