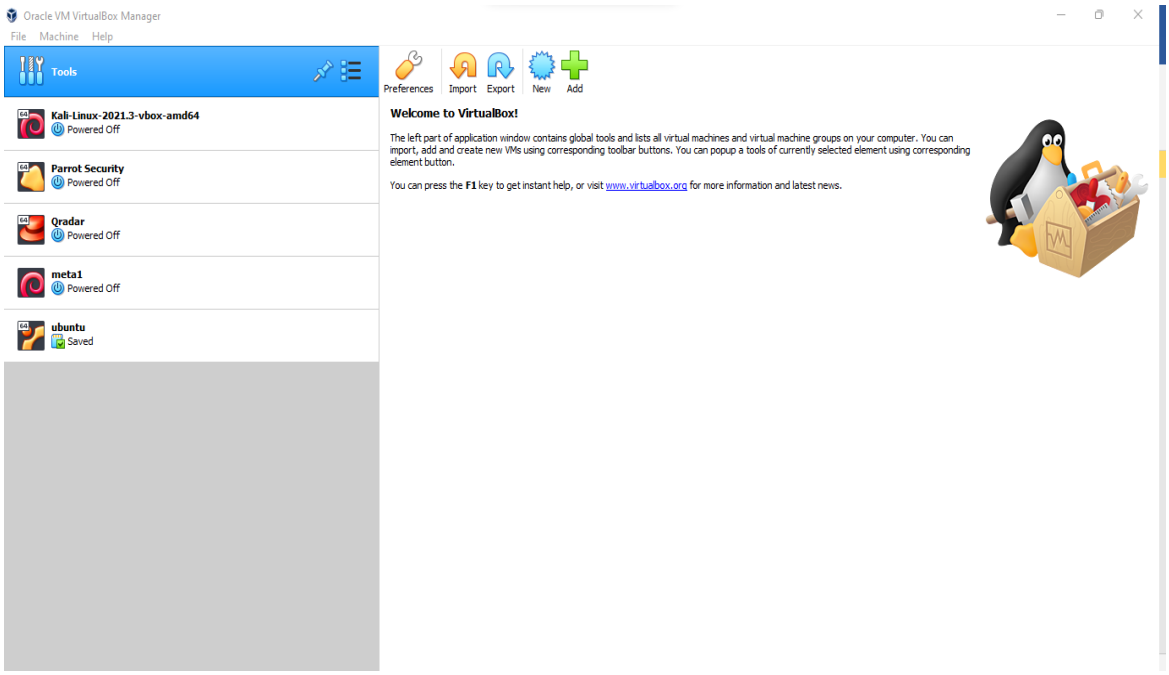
*Onboarding Linux log sources*

Step-1

- https://www.virtualbox.org/wiki/Downloas- Install virtual box in windows
- after installation: My Virtual box setup with some other configuration

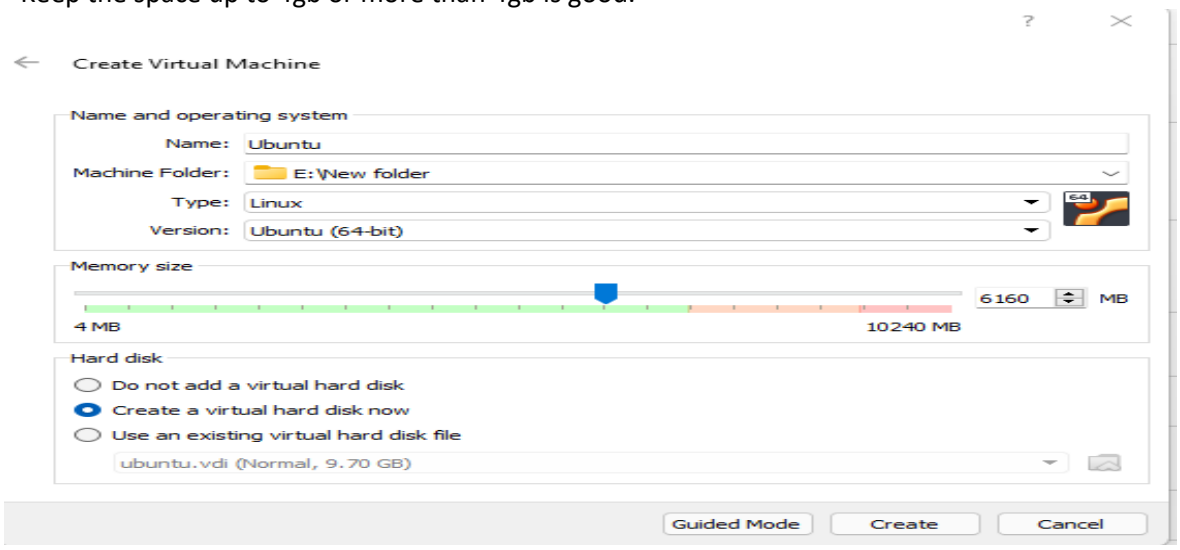



Step-2

- We have to download ubuntu server:
- https://ubuntu.com/download/server

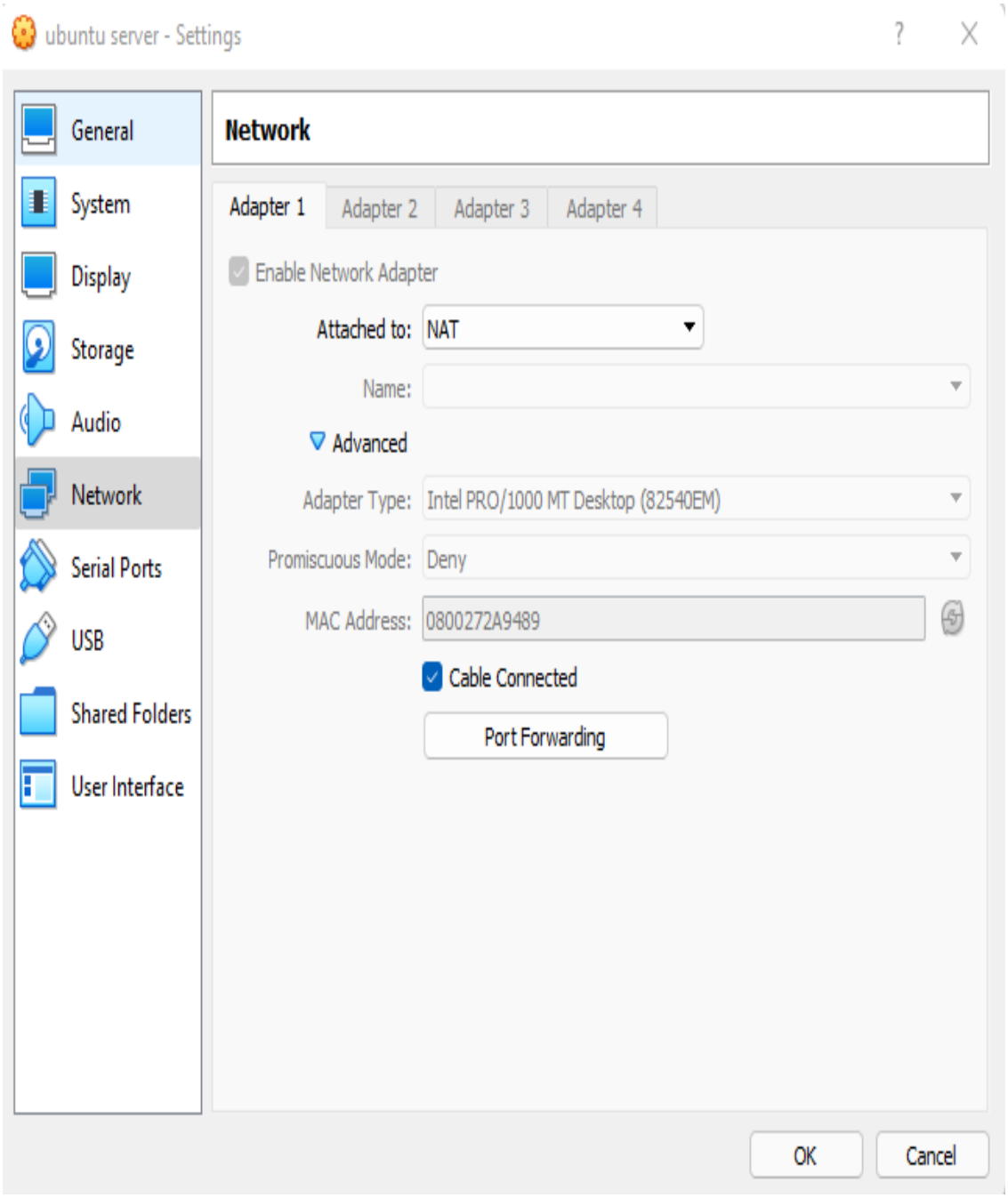
By clicking

- After downloading it, we have to configure in virtual box by selecting the file path were you downloaded the Ubuntu folder.
- Keep the space up to 4gb or more than 4gb is good.



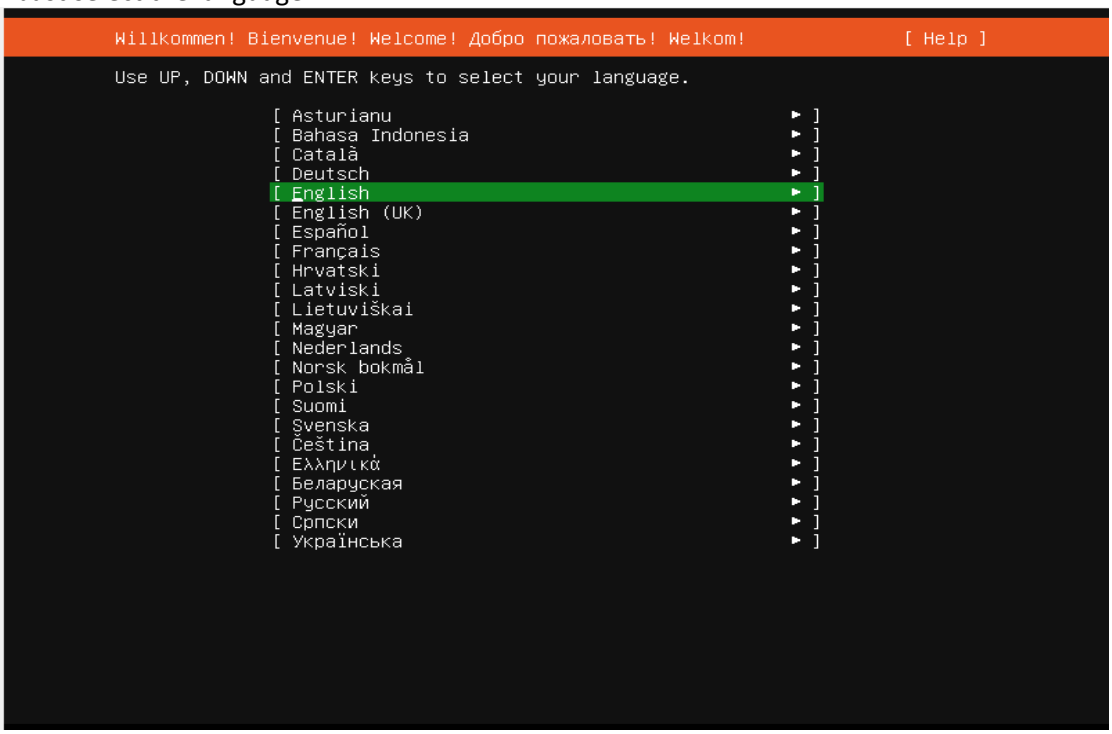
Steps-3

- We have to set the Nat network and select ok

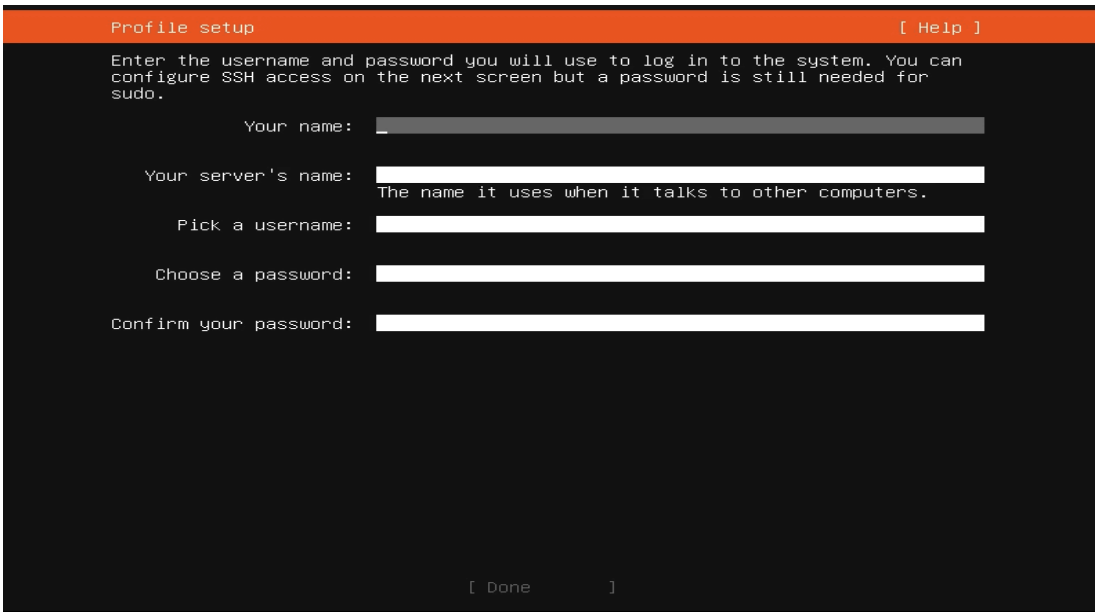


Step-4

- Start the Ubuntu in virtual box
- Just select the language

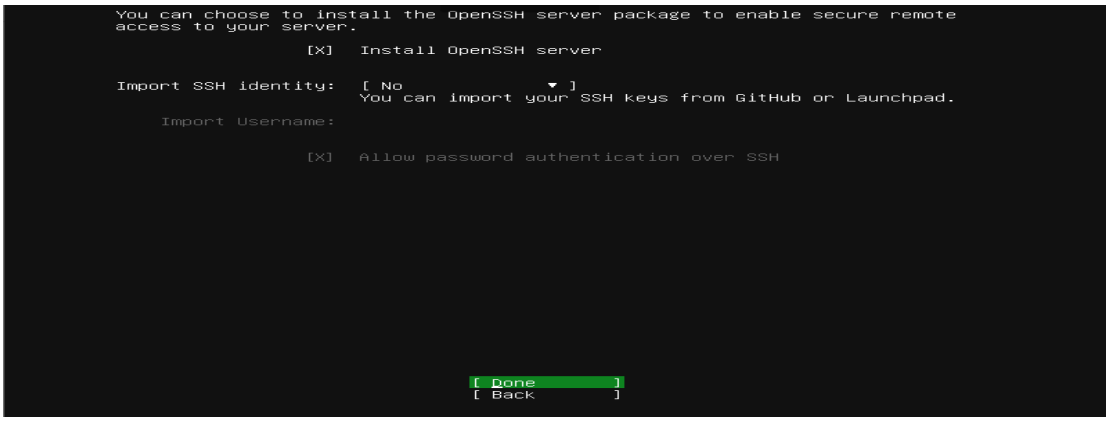



- Just go selecting done option
- Until profile setup comes.
- Set the Profile setting



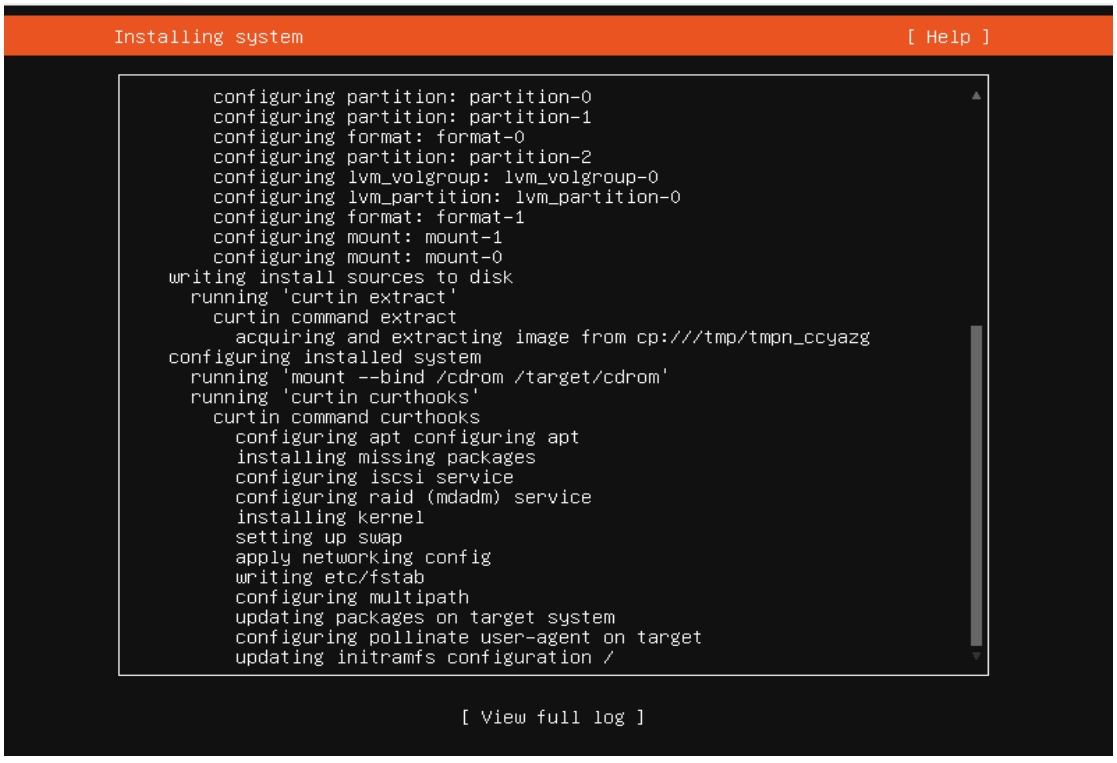
Step-4

- We have to set up ssh connection by using spacebar




Step-5

- Installation



Step-6

- We have to login using our given credential in profile setup

```
vijay login: vijay
Password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0
```

After login

Step-7

- update and upgrade Ubuntu server
- By giving commands
- Sudo apt update
- Sudo apt upgrade

```
vijay@server:~$ sudo apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
42 packages can be upgraded. Run 'apt list --upgradable' to see them.
vijay@server:~$ _
```

```
vijay@server:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  alsa-ucm-conf cloud-init cloud-initramfs-copymods cloud-initramfs-dyn-netconf libasound2
  libasound2-data libdrm-common libdrm2 libnetplan0 libnss-systemd libpam-modules
  libpam-modules-bin libpam-runtime libpam-systemd libpam0g libprocps8 libssl1.1 libsystemd0
  libudev1 libudisks2-0 linux-base netplan.io open-vm-tools openssl overlayroot procps
  python-apt-common python3-apt python3-software-properties python3-update-manager rsync snapd
  software-properties-common systemd systemd-sysv systemd-timesyncd ubuntu-advantage-tools udev
  udisks2 update-manager-core update-notifier-common wget
42 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 42.9 MB of archives.
After this operation, 1,146 kB of additional disk space will be used.
Do you want to continue? [Y/n] y_
```

Step-8

- Install fire wall-command- sudo apt install ufw
- Allow ssh connection- command -sudo ufw allow ssh
- Restart ufw- command- sudo service ufw restart

```
vijay@server:~$ sudo apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6ubuntu1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
vijay@server:~$ _
```

```
vijay@server:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
vijay@server:~$ _
```

```
Rules updated (v6)
vijay@vijay:~$ sudo service ufw restart
vijay@vijay:~$ _
```

Step-9

- We need to install ifconfig – command-sudo apt install net-tools

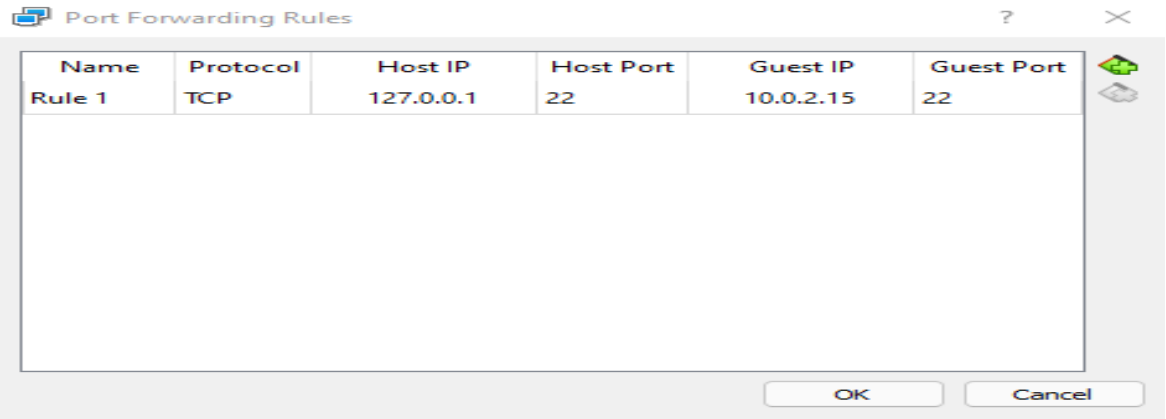
```
ijay@vijay:~$ sudo apt install net-tools
[sudo] password for vijay:
eading package lists... Done
uilding dependency tree
eading state information... Done
he following NEW packages will be installed:
  net-tools
 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
eed to get 196 kB of archives.
fter this operation, 864 kB of additional disk space will be used.
et:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e
ubuntu1 [196 kB]
etched 196 kB in 1s (351 kB/s)
electing previously unselected package net-tools.
(Reading database ... 71607 files and directories currently installed.)
reparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
npacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
etting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
rocessing triggers for man-db (2.9.1-1) ...
ijay@vijay:~$
```

- Then type -command-ifconfig

```
vijay@vijay:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fedd:a660  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:dd:a6:60  txqueuelen 1000  (Ethernet)
        RX packets 128135  bytes 191833861 (191.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15479  bytes 974036 (974.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 154  bytes 13314 (13.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 154  bytes 13314 (13.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

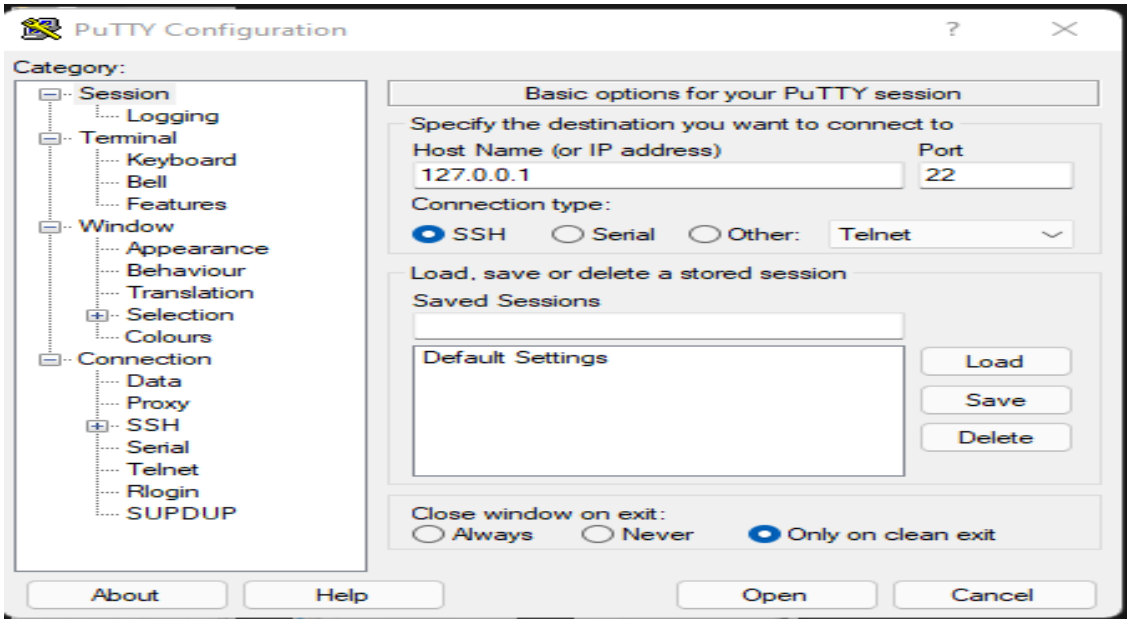
Step-10

- Go to virtual box
- Ubuntu -Settings-network-port Forwarding
- Add the ssh port number 22
- Add loop back as Host Ip-127.0.0.1 and Guest Ip -10.0.2.15 of your Ubuntu system

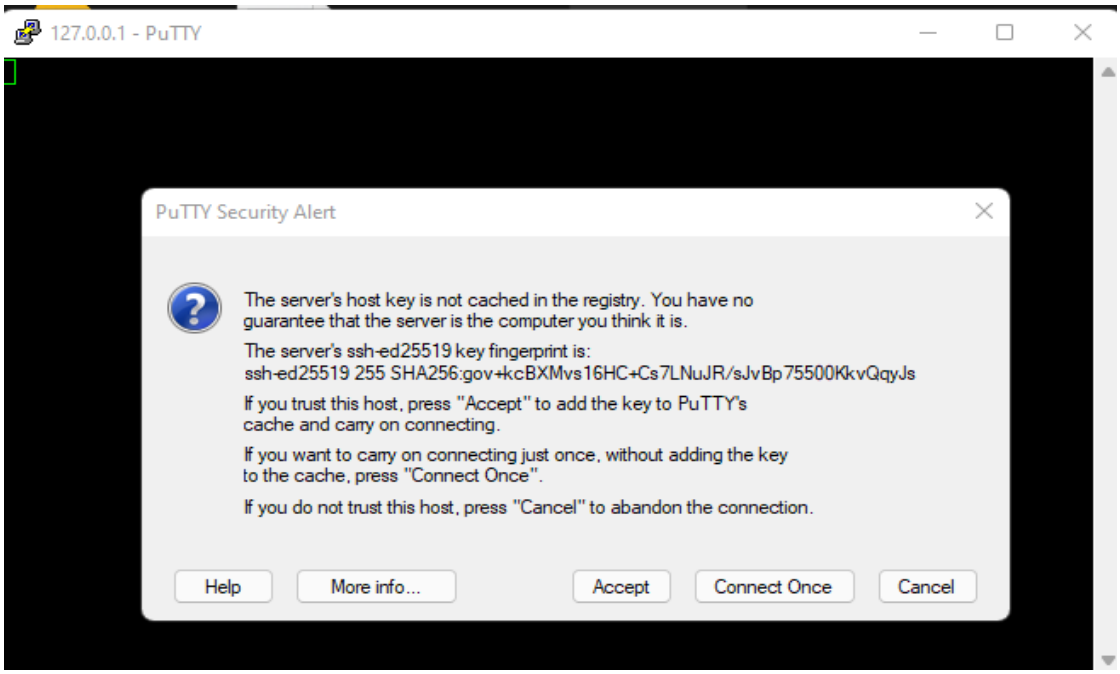



Step-11

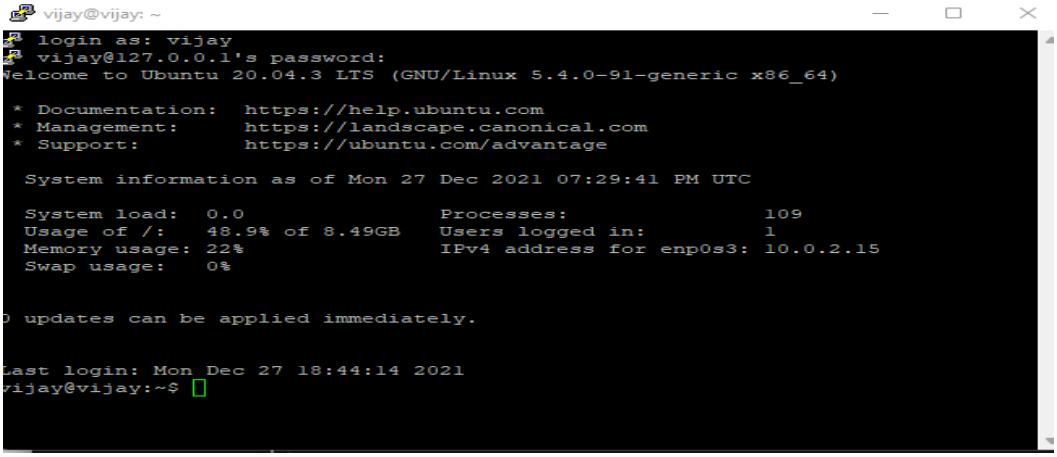
- Go to putty and give loopback Ip of ubuntu and port number 22(ssh) and open



- Select Accept option




- Login




Step-12

- https://www.splunk.com/en_us/download/universal-forwarder.html
- Log in to splunk website to copy command to install splunk forwarder
- wget -O splunkforwarder-8.2.4-87e2dda940d1-Linux-x86_64.tgz 'https://download.splunk.com/products/universalforwarder/releases/8.2.4/linux/splunkforwarder8.2.4- 87e2dda940d1-Linux-x86_64.


Step-13

- Copy it in putty -command-cd /opt-copy the link

```
vijay@server:/opt$ sudo wget -O splunk-8.2.4-87e2dda940d1-linux-2.6-x86_64.rpm 'https://download.splunk.com/products/splunk/releases/8.2.4/linux/splunk-8.2.4-87e2dda940
d1-linux-2.6-x86_64.rpm'
[sudo] password for vijay:
--2021-12-26 12:47:26--  https://download.splunk.com/products/splunk/releases/8.2.4/linux/splunk-8.2.4-87e2dda940d1-linux-2.6-x86_64.rpm
Resolving download.splunk.com (download.splunk.com)... 18.67.161.119, 18.67.161.51, 18.67.161.26, ...
Connecting to download.splunk.com (download.splunk.com)|18.67.161.119|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 570822458 (544M) [binary/octet-stream]
Saving to: 'splunk-8.2.4-87e2dda940d1-linux-2.6-x86_64.rpm'

splunk-8.2.4-87e2dda940d1-linux-2.6-x86_6  60%[=============================================>                    ] 327.11M  6.24MB/s    eta 34s
```

- Extract the file- command-cd/opt-sudo tar xvzf splunkforwarder-8.2.4-87e2dda940d1-Linux-x86_64.tgz
- We will get a file splunkfowarder

```
root@server:/opt# ls
splunk-8.2.4-87e2dda940d1-linux-2.6-x86_64.rpm  splunkforwarder-8.2.4-87e2dda940d1-Linux-
splunkforwarder                                 splunkforwarder-8.2.4-87e2dda940d1-Linux-
```

- Splunk installed
- Then we have to start the splunk going to bin in splunkforwader – sudo ./splunkstart

Step-14

- Create Inputs.conf and output.conf-
- Commands
- cd /opt/splunkforwader/etc/system/local

```
vijay@vijay:/opt$ cd splunkforwarder/etc/system/local
vijay@vijay:/opt/splunkforwarder/etc/system/local$ ls
README  server.conf
vijay@vijay:/opt/splunkforwarder/etc/system/local$
```

- sudo vi inputs.conf

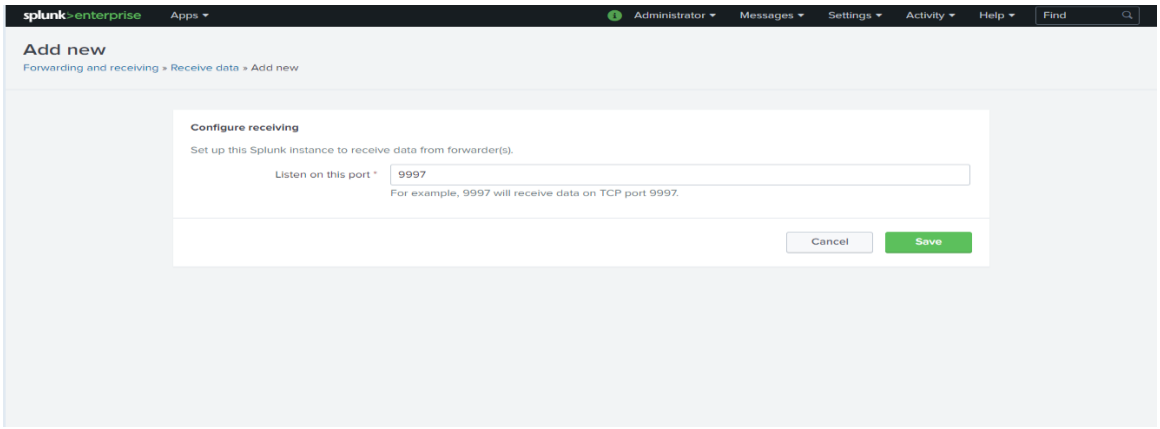
```
vijay@vijay:/opt/splunkforwarder/etc/system/local$ cat input.conf
[monitor:///var/log/auth.log]
disabled =false
sourcetype = linux_logs
index = linux
```

- Sudo vi output.conf
- We have to give window host IP address

```
ijay@vijay:/opt/splunkforwarder/etc/system/local$ cat output.conf
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.0.102:9997

[tcpout-server://192.168.0.102:9997]
```

Step-15

- Now go the splunk web interface which you already created in windows-add port number 9997for receiving in-(path)-Setting-Forwarding and Receving.
- Create index with name of linux

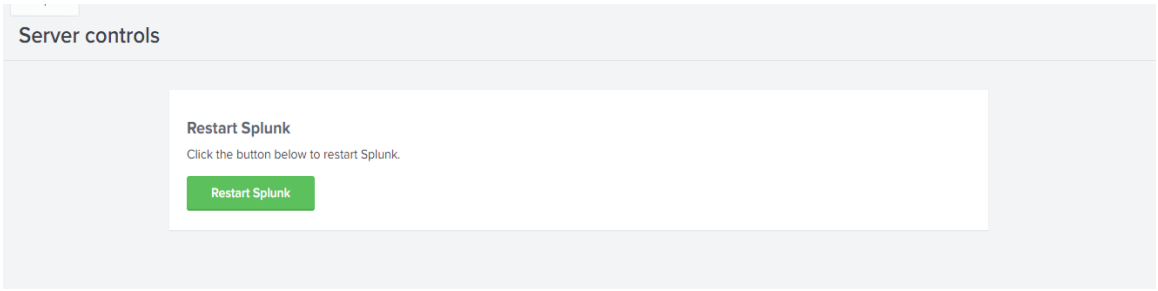



Step-16

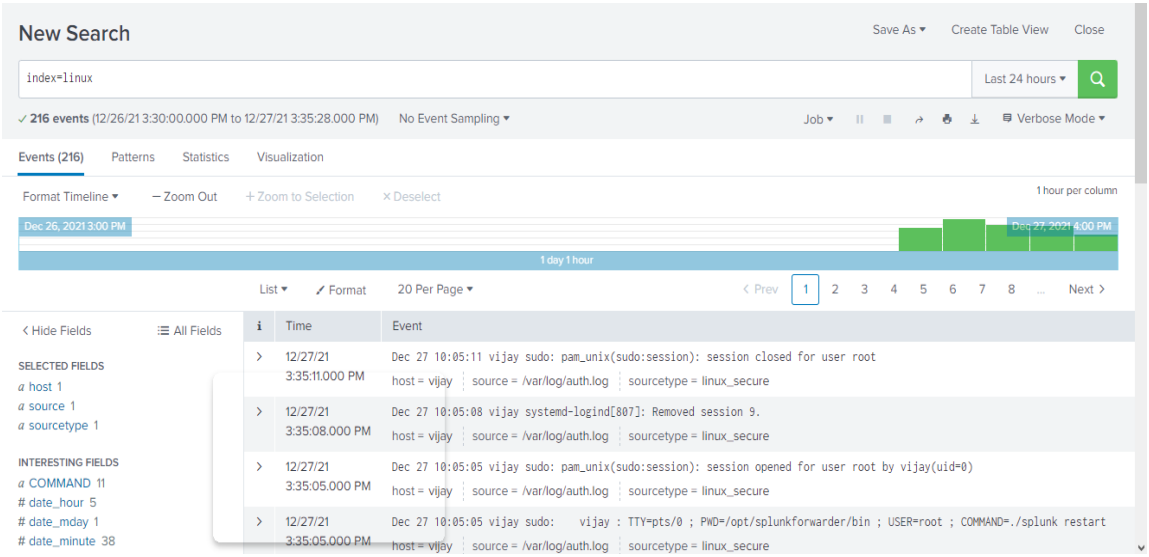
- Come back to opt folder in Ubuntu using command – cd ..
- Again go to bin in opt folder -cd bin
- Then restart the splunk – command – sudo ./splunk restart

```
vijay@vijay:/opt/splunkforwarder/bin$ sudo ./splunk restart
[sudo] password for vijay:
splunkd 19053 was not running.
Stopping splunk helpers...

Done.
Stopped helpers.
Removing stale pid file... done.
splunkd is not running.

Splunk> 4TW

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

- Also restart splunk web interface-(path)-setting-server controls-restart




- Again login web interface go to search index give query -index=linux




- Now we are receiving the logs from linux (Ubuntu server)