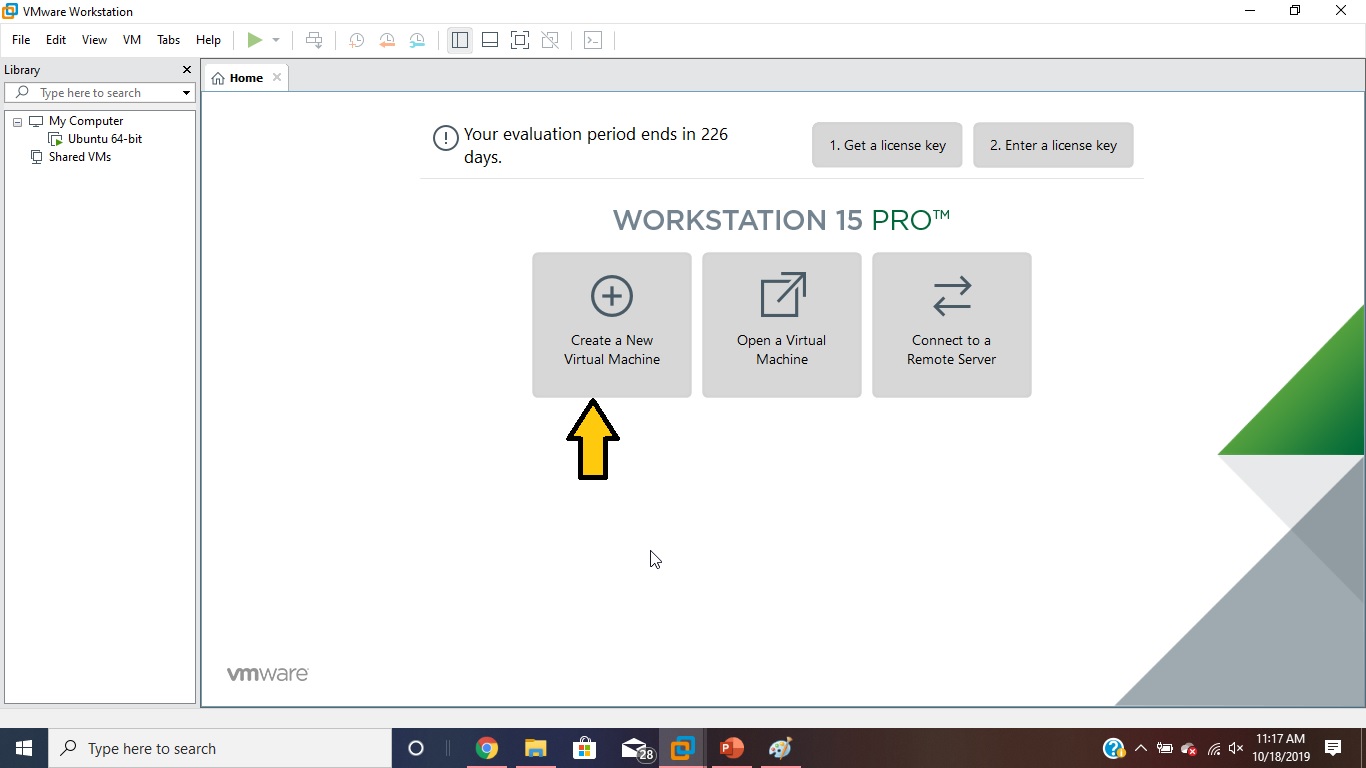
Patrick Morley

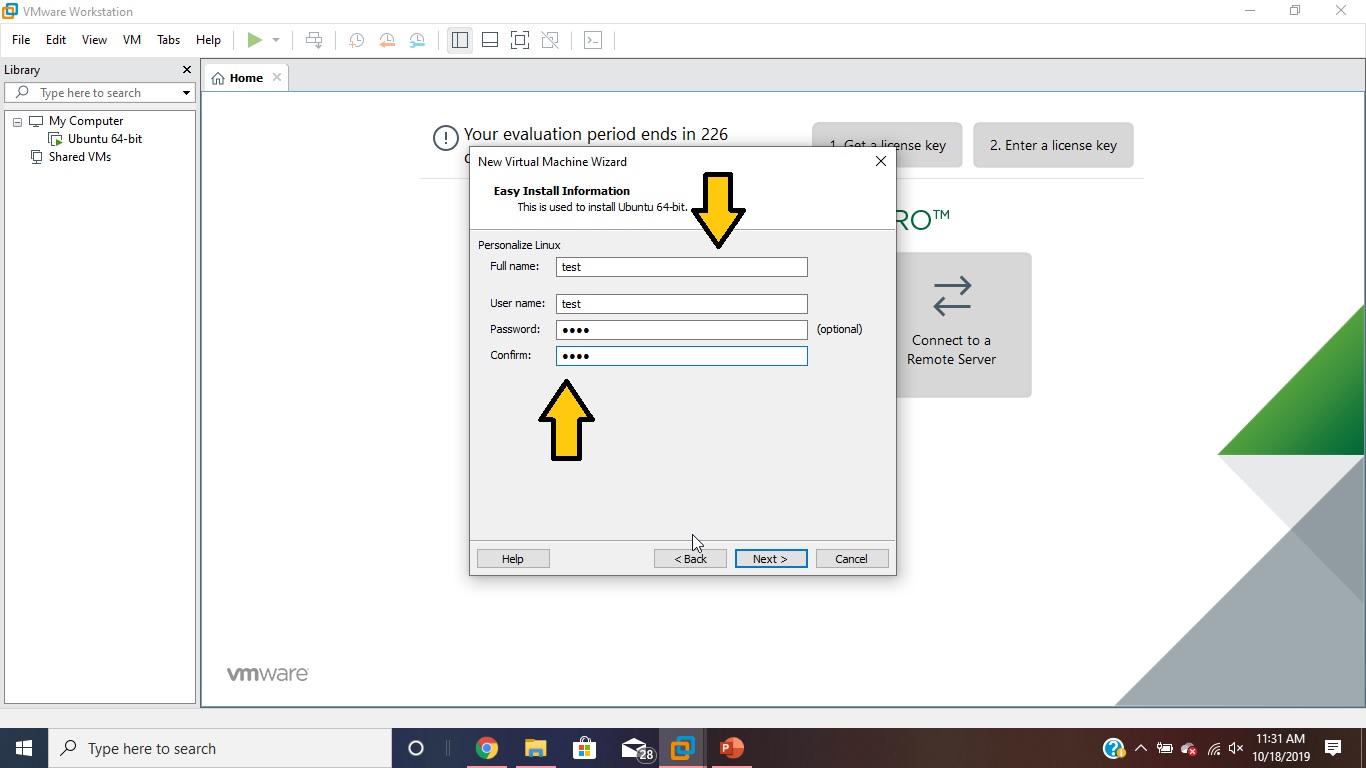
Professor Holden-Gouveia

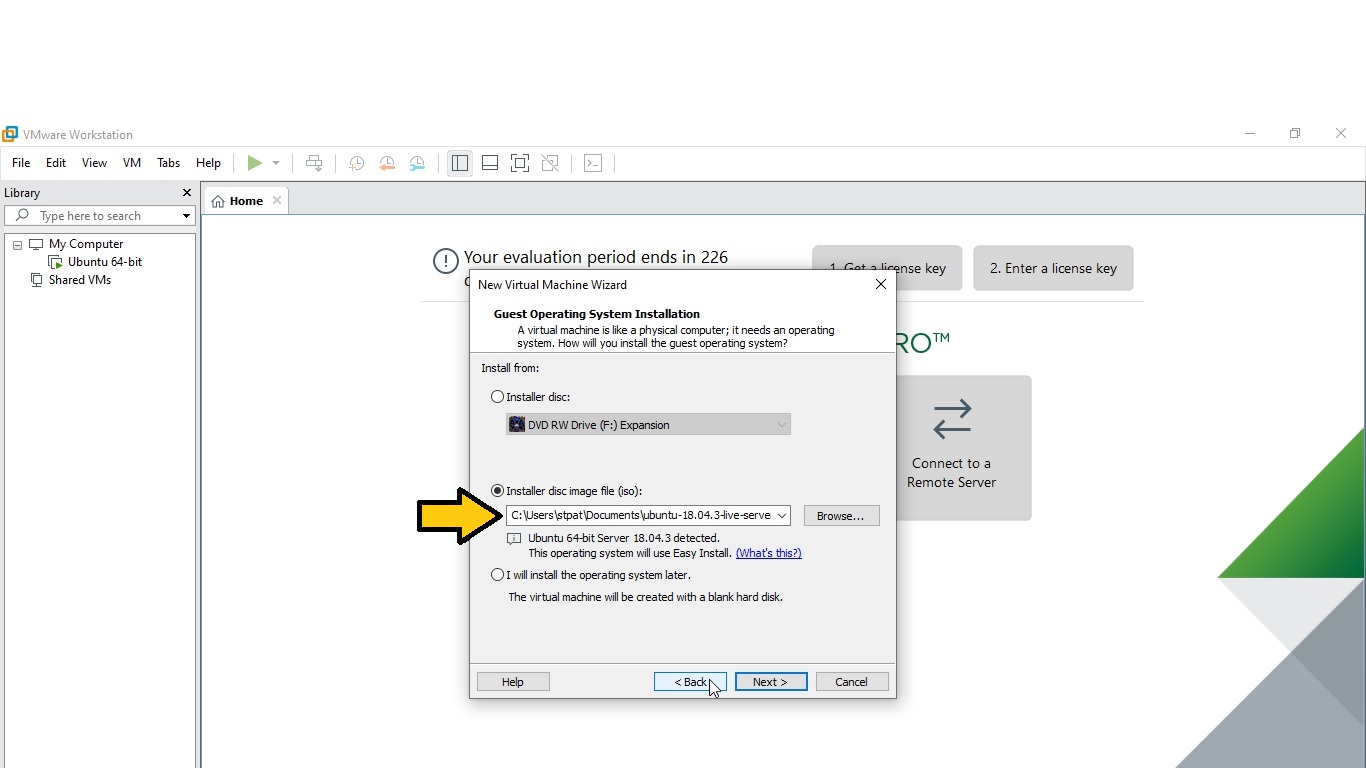
Linux Administration

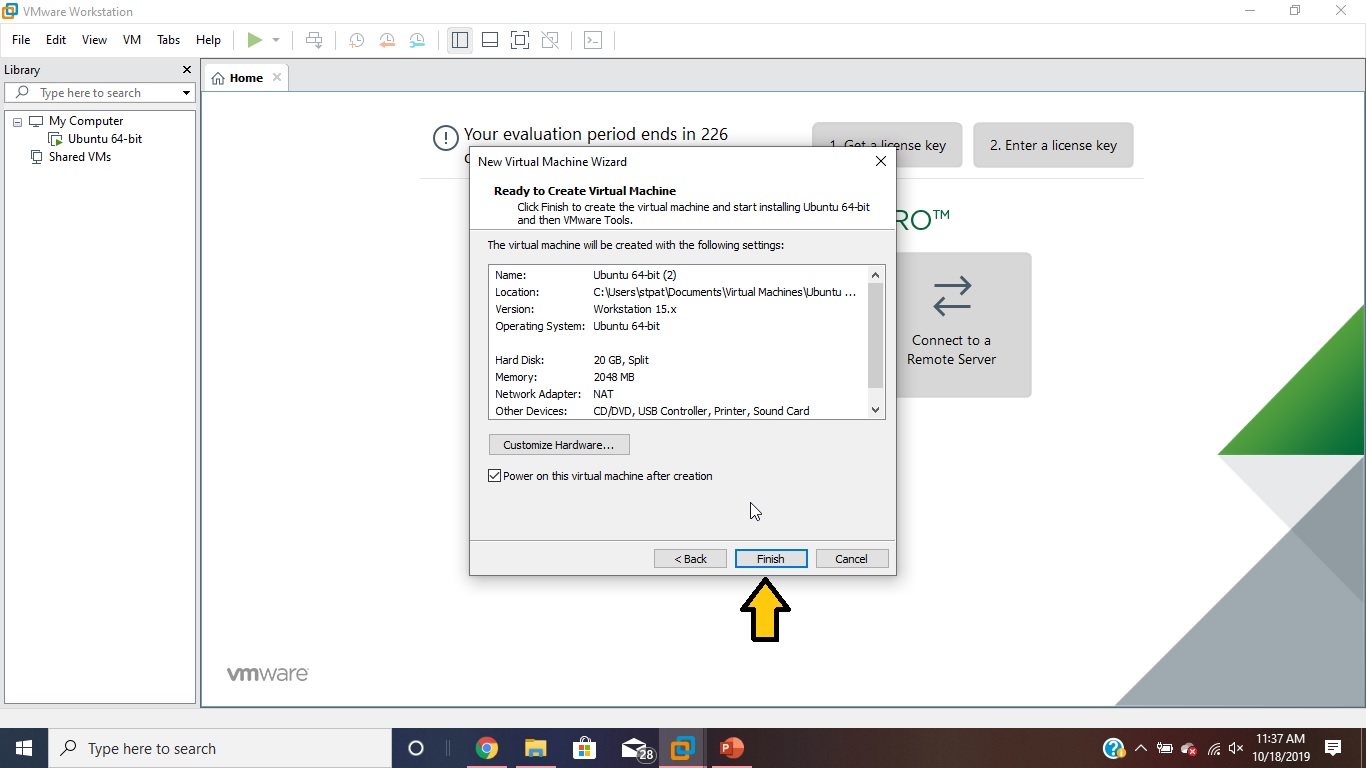
Ubuntu Documentation

First, I set up my Ubuntu server on VMware on my laptop. I downloaded and set up the Ubuntu desktop first, before I realized it was the wrong one. I started off by going to the Ubuntu website and downloading the Ubuntu server. Then I started up the VMware workstation and selected new machine. I chose the Ubuntu ISO file I had downloaded and followed the prompts till it was fully installed. I created a username and password on the first startup.





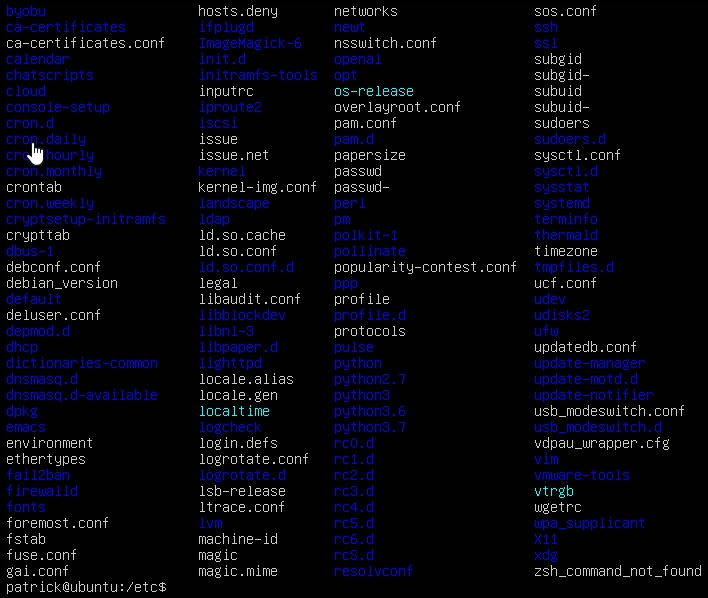




**Ubuntu: starts at the directory labeled patrick**







/etc/passwd: navigate to the etc directory with ‘cd /etc’ (passwd file located here)

/etc/shadow: navigate to the etc directory with ‘cd /etc’ (shadow file located here)

/etc/group: navigate to the etc directory with ‘cd /etc’ (group file located here)

/etc/login.defs: navigate to the etc directory with ‘cd /etc’ (login.defs file located here)

/etc/adduser.conf: navigate to the etc directory with ‘cd /etc’ (adduser.conf file located here)

/etc/sudoers: navigate to the etc directory with ‘cd /etc’ (sudoers file located here)

/etc/motd: navigate to the etc directory with ‘cd /etc’ (motd file located here)

/etc/skel: navigate to the etc directory with ‘cd /etc’ (skel file located here)

/bin: Change directory with ‘cd /’ (bin directory located here)

/etc: Change directory with ‘cd /’ (etc directory located here)

/home: Move up one directory with ‘cd ..’ (this is the home directory)

/opt: Change directory with ‘cd /’ (opt directory located here)

/tmp: Change directory with ‘cd /’ (tmp directory located here)

/usr: Change directory with ‘cd /’ (usr directory located here)

/var: Change directory with ‘cd /’ (var directory located here)

/var/log/messages: cd /var/log cat syslog

/var/log/auth.log: cd /var/log cat auth.log

/var/log/boot.log: I could not find a boot.log. One website said there hasn’t been a boot.log since Ubuntu 16.04, another site said it gets appended to syslog. I checked syslog but couldn’t find anything about boot. I found that using journalctl with options can give you some boot information. Journalctl comes from journald, which is a logging daemon from system.

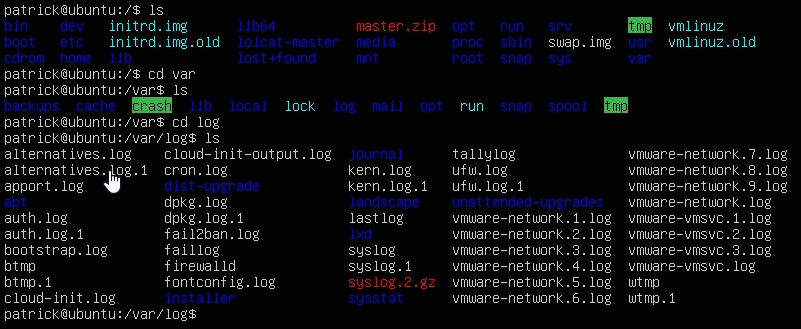
/var/log/dmesg: There is no dmesg file anymore, but you can still use the dmesg command to get output.

/var/log/kern/log: cd /var/log cat kern.log

/var/log/faillog: cd /var/log cat faillog

/var/log/cron: In order to view the cron log, I had to use vi /etc/rsyslog.d/50-default.conf and remove the # from in front of cron. Then sudo service rsyslog restart and sudo service cron restart.

/var/log/yum.log: Ubuntu does not use yum. I tried to find a way to install it on Ubuntu but no luck. Ubuntu uses apt-get. You can find these files in cd /var/log/apt.



**Repositories:**

List repositories: grep ^[^#] /etc/apt/sources.list or sudo grep -Erh ^deb /etc/apt/sources.list\*

^[^#] suppresses comments. /etc/apt/sources.list.d is the directory where the information is maintained.

List installed packages: sudo apt-cache policy

Before I changed anything, I used: sudo cp /etc/apt/sources.list /etc/apt/sources.list.backup to create a backup file in case I messed up and needed to recover the file.

In order to add repositories, I used: sudo vi /etc/apt/sources.list to enter the editor. Then I removed the # from 2 of the repositories to uncomment them and put them into effect.

I also used: sudo add-apt-repository “deb <http://us.archive.ubuntu.com/ubuntu/> saucy universe multiverse” to add another repository. I added a # in the editor to comment this out.

I used: lsb\_release -sc to find out what my release is. It is bionic.

I updated my system and new repositories with sudo apt-get update.

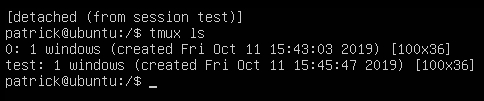
I added the PPA repository with: sudo add-apt-repository ppa:Thomas-schiex/blender and installed blender with sudo apt-get install blender. Then I removed it with: add-apt-repository –remove ppa:Thomas-schiex/blender. I then used sudo apt-get install ppa-purge and used ppa-purge ppa:Thomas-schiex/blender to fully remove it from the system. You could also manually remove it from the system with: sudo rm /etc/apt/sources.list.d/Thomas-schiex-ubuntu-blender-bionic.list

I used: sudo apt-get upgrade to upgrade my system.

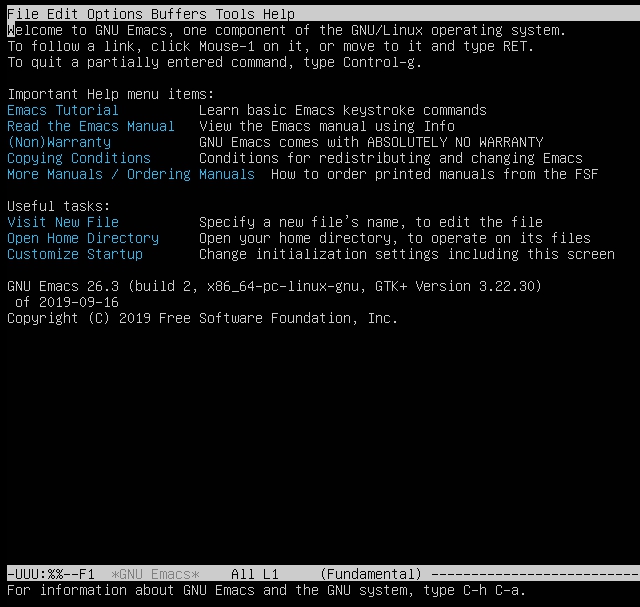
The first step I took in installing a package was to search for one. I used sudo apt-cache search rhythmbox. You can upgrade the package with sudo apt-get upgrade rhythmbox. Or you can remove the package with: sudo apt-get remove rhythmbox. Or purge it with sudo apt-get remove –purge rhythmbox.

In order to clean out your caches and get back some hard drive space you can use 2 commands. Sudo apt-get clean. Or to clean out your cache and save the newest versions of the packages you can use: sudo apt-get autoclean.

Installing Tmux was pretty easy. I just use: sudo apt-get install tmux and it was ready to use. I always use sudo apt-get update before and after I install something new and I make sure I use sudo apt-get upgrade every so often too. The command tmux starts a session. Ctrl-b d gets you out of a session. And tmux new -s test creates a new session called “test”; you can replace “test” with whatever name you want to call it.



In order to install emacs, you first have to install the ppa. Sudo add-apt-repository ppa:kelleyk/emacs. Then use sudo apt update and sudo apt install emacs26. Type the command emacs to enter the program. There is a tutorial to check out in emacs and you can navigate to the home directory. You can use the up and down arrows to navigate or use ctrl-v to move down or ctrl-b to move up.



I used sudo apt-get update && apt-get upgrade -y to ensure my system was up to date. Then I used sudo apt-get install fail2ban. Fail2ban is program that automatically seeks out attackers on your system and blocks their IP address. Once you install fail2ban it automatically starts working. If you want to make any changes to this program it’s best to create a new file: sudo cp /etc/fail2ban/fail2ban.conf /etc/fail2ban/fail2ban.local.



I used sudo apt-get install vim to upgrade vi to vim.

How to install and enable canonical-livepatch:

I registered at auth.livepatch.canonical.com to get a token (code).

I used sudo apt install snapd to install snap which is the program used to install canonical-livepatch.

Sudo snap install canonical-livepatch

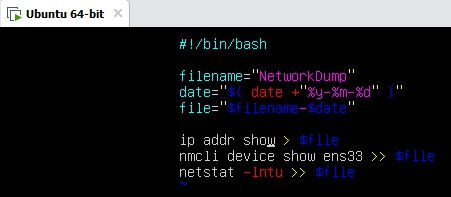
Sudo canonical-livepatch enable xxxxc4xxxx67xxxxbxxxxfbxx4e (not my real token)

Sudo canonical-livepatch status

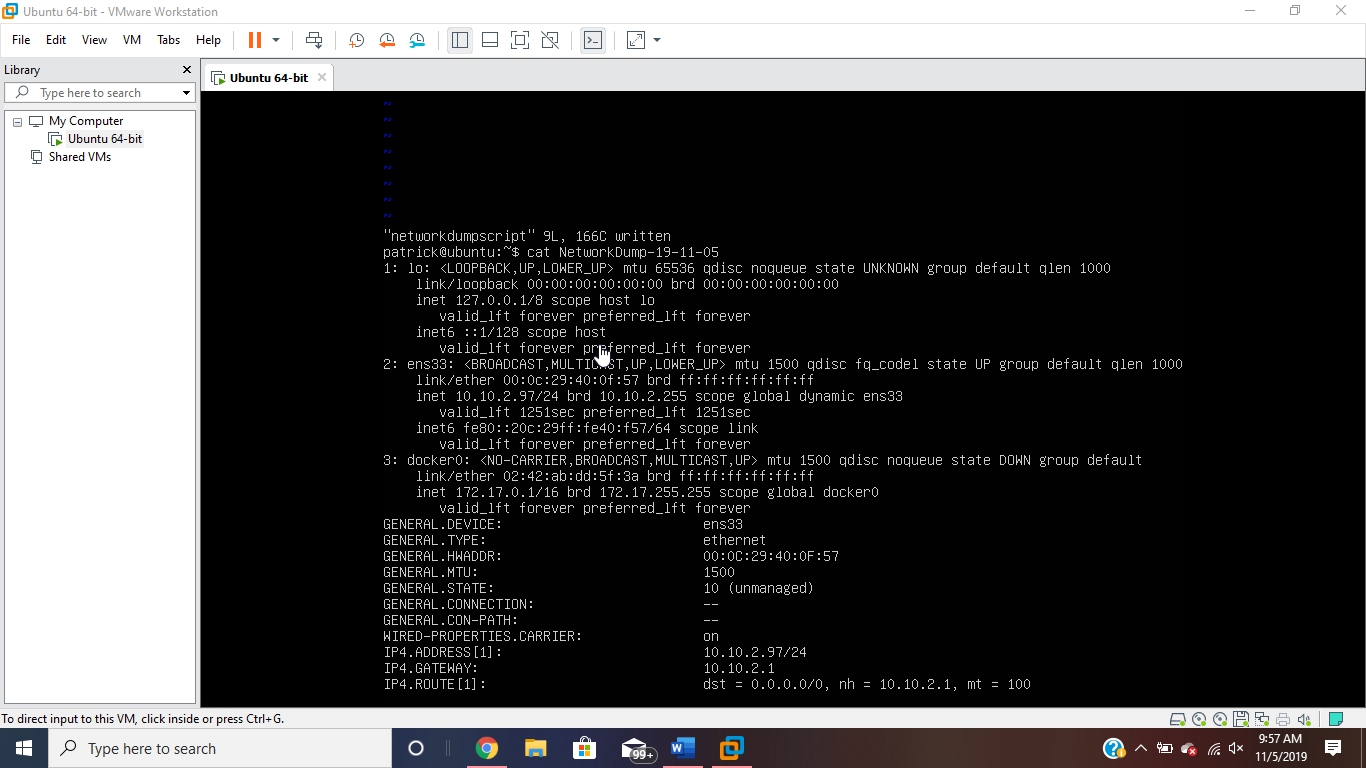
Ip addr show

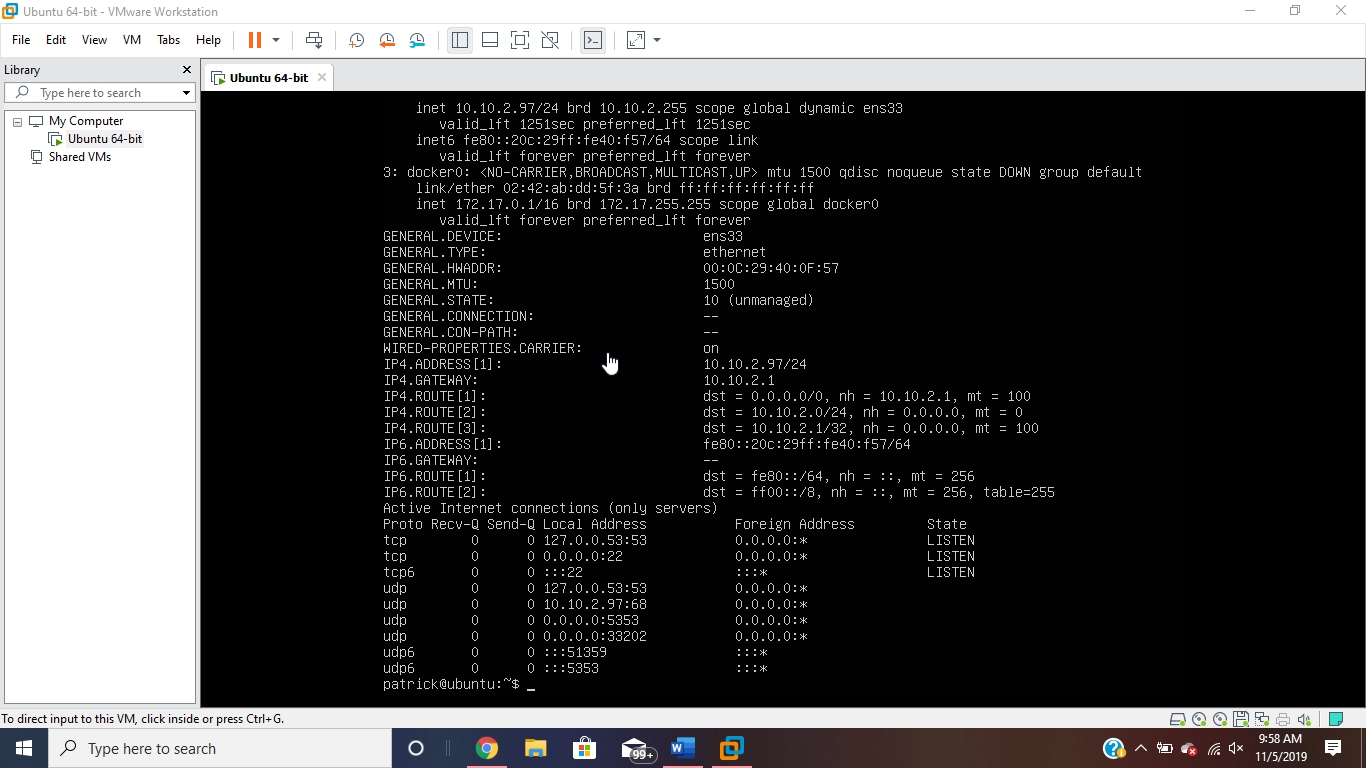
Nmcli device show ens33

Netstat -lntu









Sudo apt install firewalld (Install firewalld command)

Sudo firewall-cmd –state = running

Sudo firewall-cmd –permanent –add-port=80/tcp (Open port 80 permanently)

Sudo firewall-cmd –permanent –add-port=443/tcp (Open port 443 permanently)

Sudo firewall-cmd --reload

Sudo firewall-cmd –list-all

Sudo firewall-cmd –zone=public –add-service=http

Sudo firewall-cmd –zone=public –add-service=https

Sudo firewall-cmd –runtime-to-permanent

Sudo apt install iptables (install iptables)

Sudo iptables -L -v (list iptables rules, add –line-numbers to add line numbers for each rule)

Sudo iptables -L | grep policy

Sudo iptables –policy INPUT ACCEPT (This sets Accept as default)

Sudo iptables –policy OUTPUT ACCEPT

Sudo iptables –policy FORWARD ACCEPT

Sudo iptables –policy INPUT DROP (This sets Deny as default)

Sudo iptables –policy OUTPUT DROP

Sudo iptables –policy FORWARD DROP

Sudo /sbin/iptables-save

-t (tables: filter, mangle, nat, raw)

-A (append, to Input or Output)

-D (delete rule)

-s (source, ip address)

-d (destination, ip address, 59.45.175.62 for specific ip, 59.45.175.0/24 for all ip)

-j (used to Accept, Drop, or Reject)

Input (select a certain line)

-F (flushes a chain)

-I (inserts rules on a specific line)

-R (replaces rule)

-p (specifies protocol to be used, tcp)

-m (selects the module, tcp)

--dport (checks the destination port, 22)

Multiport (selects multiple ports, 22, 5901)

--icmp-type (17)

Conntrack (connection tracking module)

--ctstate (sets the states, Related, Established)

-P (changes the default policy)

-i (input interface for loopback interface (lo) if chain empty, -I to adds it to the top)

-o (output interface for loopback (wlan0))

! (negates operator)

--tcp-flags (“mask” Syn, Fin “compared flags” Syn, Fin)

Limit

Recent

Owner

-N (create custom rule)

Log

Iptables-save (saves rules)

Iptables-restore (applies rules)

Sudo apt install iptables-persistent

Sudo iptables -A INPUT -I eth0 -p tcp -m tcp –dport 3306 -j ACCEPT

Sudo iptables -A INPUT -I eth0 -p tcp –dport 22 -j ACCEPT