LINUX INSTALLATION of ISO :

Download virtual box -> Download linux iso image -> in virtual

server

press new symbol

button -> attach the iso image -some configuration's -> set user

name and password -> some configuration's ->set root password and user

name and user password -> after configuration completed enter into root in hostname -> root password

How to Enable IP Address?

if IP Address is not working disable and enable

your server.

command

in network script:

cd /etc/sysconfig/

cd network-scripts/

ls

Vi ifup ifcfg-enp0s3

(Yes)

Disable:

ifdown ifcfg-enp0s3

Enable:

ifup ifcfg-enp0s3

ip a (To check ip address)

To Restart the server:

systemctl restart network

To Restart Total Server:

init 6

How to start putty , Winscp and FTP:

Enable in Setting - Nat Gate to Bridge Option

->Linux server -> type = cd /etc/sysconfig/ -> ls -> cd network-scripts/ ->

ls->vi ifup ifcfg-enp0s3

(Yes) enable -->ip a ->ping and check

If not working means Disable and Enable the IP Address.

Disable:

ifdown ifcfg-enp0s3

Enable:

ifup ifcfg-enp0s3

ip a (To check ip address)

To Restart the server:

systemctl restart network

To Restart Total Server:

init 6

Your Local IP adress and your server IP Address -> open putty and attach

your server IP Address -> your host name -> root

- **➔ root password**
- **➔ yum install vsftpd -y**

Step 3. Open the configuration file of vsftp server and disable anonymous access by
default ftp is set to anonymous access:

-> vi /etc/vsftpd/vsftpd.conf

Change the following values to the value shown below:

anonymous_enable=NO

Add the following parameters in the end of the file. these two parameters

will provide security to your ftp server.

chroot_local_user=YES
allow_writeable_chroot=YES

Save and Exit
:wq

Step 4. Create user for ftp access

useradd ftpuser

passwd ftpuser

Step 5. Start and enable the service

systemctl start vsftpd

systemctl enable vsftpd

Step 6. Apply the firewall rule

firewall-cmd --permanent --zone=public --add-service=ftp

firewall-cmd --reload

Step 7. Set selinux boolean on 搘tpd_full_access

setsebool -P ftpd_full_access on

->Go FTP Client ->FileZilla ->Enter Your server IP adress ->FTP User Name
-> FTP Root -> password -> port no-> 22

Output : Sucess

-> Go to winscp and choose SMPT ->Type your server IP adress -> RootPassword

-> CONNECT.

To Trasfer the file and start process in your putty server with your commands

according to your process.

if IP Address is not working disable and enable your server.

in network script:

command

cd /etc/sysconfig/

cd network-scripts/

Disable:

ifdown ifcfg-enp0s3

Enable:

ifup ifcfg-enp0s3

How to Install Web Apache?

yum install httpd

Start the server, and configure it to start after

system reboots:

service httpd start

chkconfig httpd on

Check for configuration errors:

service httpd configtest

Create firewall rules to allow access to the ports on which the HTTP server listens, for example:

iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT

service iptables save

How to Set Static IP ADDRESS ?

- **cd /etc/sysconfig/network-scripts**
- **ls**
- **vi ifcfg-eth0**

 # DHCP configration for eth0

- **TYPE=Ethernet**
- **PROXY_METHOD=none**
- **BROWSER_ONLY=no**
- **BOOTPROTO=none**
- **IPADDR=192.168.42.10 (Your System IP Address)**
- **PREFIX=24**
- **GATEWAY=192.168.42.129 (Your System Gateway IP Address)**
- **DNS1=192.168.42.129 (Your System DNS1 IP Address)**
- **DEFROUTE=yes**
- **IPV4_FAILURE_FATAL=no**
- **IPV6INIT=no**
- **IPV6_AUTOCONF=yes**
- **IPV6_DEFROUTE=yes**
- **IPV6_FAILURE_FATAL=no**
- **IPV6_ADDR_GEN_MODE=stable-privacy**
- **NAME=enp0s3**
- **UUID=20c61324-5443-4751-938b-dc367d7ec6fe**
- **DEVICE=enp0s3 (Your Server ID)**
- **ONBOOT=yes**

Wq!

systemctl restart network

UBUNTU INSTALLATION of ISO :

LINK TO DOWNLOAD ISO IMAGE:

https://cdimage.ubuntu.com/releases/22.04/release/

INSTALLATION of ISO :

Download virtual box -> Download linux iso image -> in virtual

server

press new symbol

button -> attach the iso image -some confiuguration's -> set user

name and password -> some configuration's ->set root password and user

->change root password and user root user name -> after configuration completed enter into root in hostname -> username(dharaka)->username password ->su ->root password.

ubuntu@localhost:~$ sudo -s

[sudo] password for ubuntu: # input self password

root@localhost:/home/ubuntu# # just switched

[2] Or it's possible to switch to root account with standard su command to set root account's password.

ubuntu@localhost:~$ sudo passwd root

[sudo] password for ubuntu: # input self password

New password: # set root password

Retype new password: # confirm

passwd: password updated successfully

ubuntu@localhost:~$ su -

Password: # input root password

root@localhost:~# # just switched

*****

The examples on this site shows by root user account. If you use Sudo, add [sudo] on the

head of commands.

It's better to restrict users who can [su] to root if you enable root account like

follows. For using by Sudo, it's possible to limit to prohibit shells in sudoers config,

refer to details about Sudo Settings.

[3] For [su] command restriction, set like follows.

root@localhost:~# vi /etc/pam.d/su

 # line 15 : uncomment and add a group which is allow to run [su] command

auth required pam_wheel.so group=adm

auth required pam_wheel.so group=adm (Change)

 # add an user you allowed to run [su] to the group you set above

root@localhost:~# usermod -aG adm ubuntu

putty -> Attach IP -> host name -> user name ->user Password -> su -> root password