ASSIGNMENT

Systems and Network Programming -IE2012

RAJASOORIYA D.G.C.H.

Y2.S1.WD.CS.01.02

MALABE CAMPUS

05/10/2024

Table of Contents

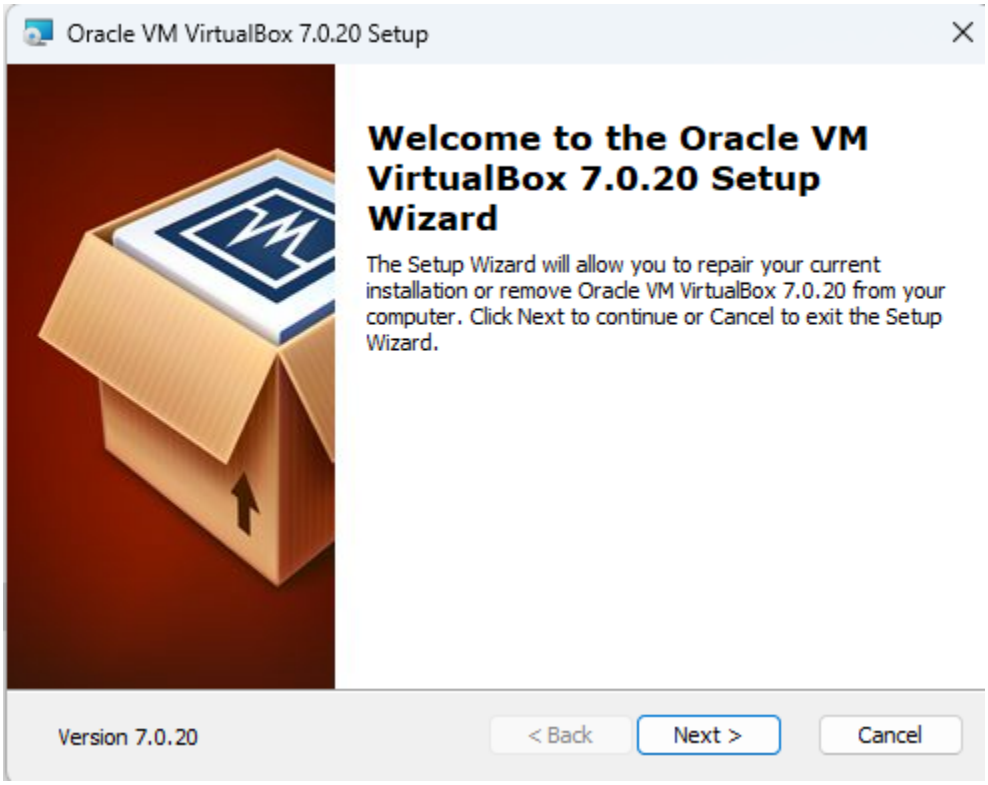
1.Basics Linux Environments

Virtual Machine Setup

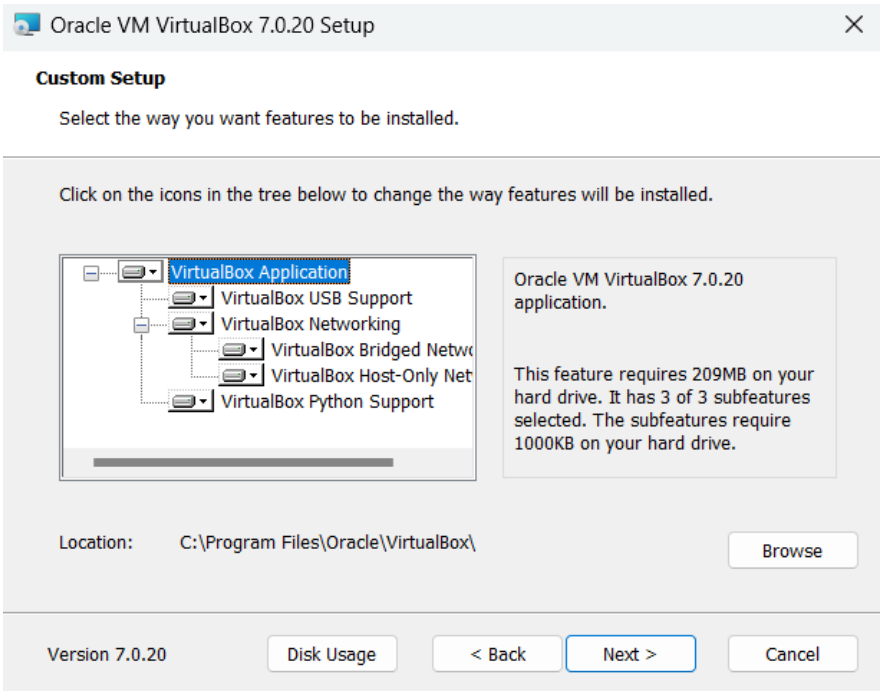
Step 1: Download the virtual emulator first. I used Oracle VirtualBox. This is the official website to download VM.

https://www.virtualbox.org/wiki/Downloads

Step 2: After downloaded double click on that file to start installation. Accept the license agreement.

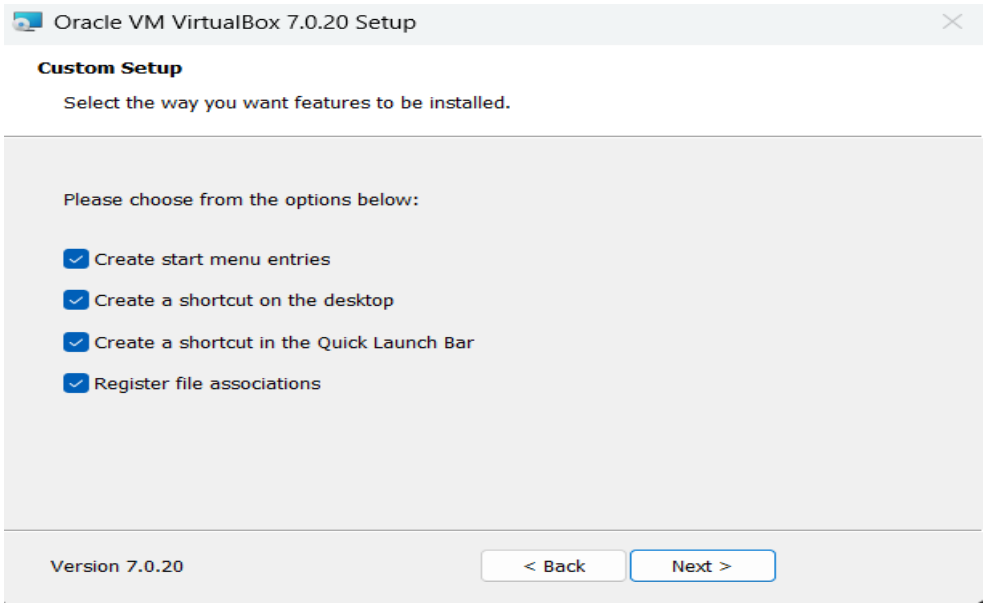


Step 3: Choose the installation directory. If you do not have a proper reason to change leave as default.

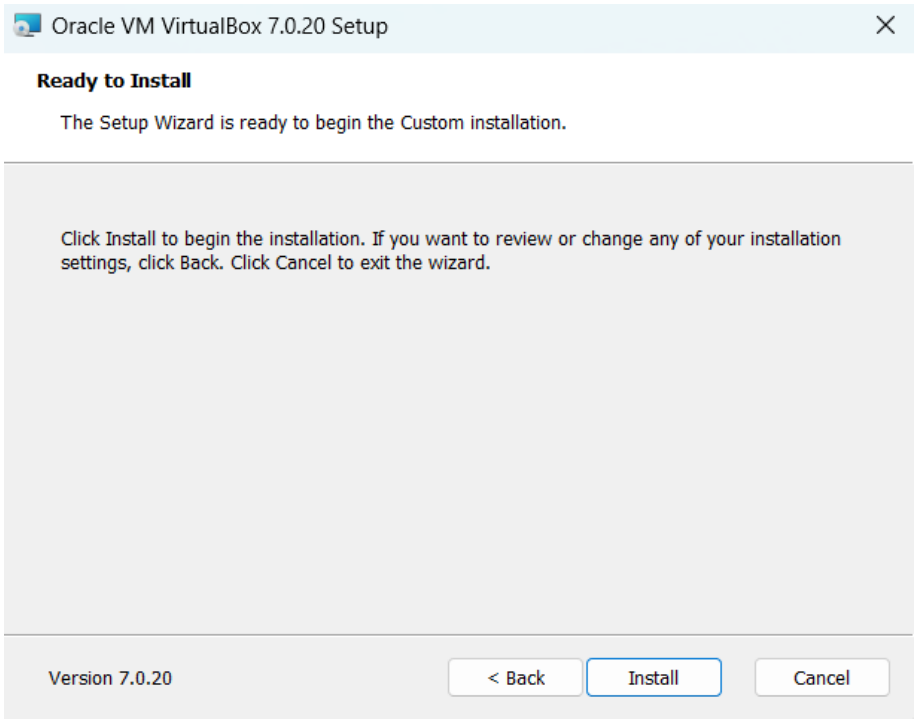


Step 4: Select the component to install.

.

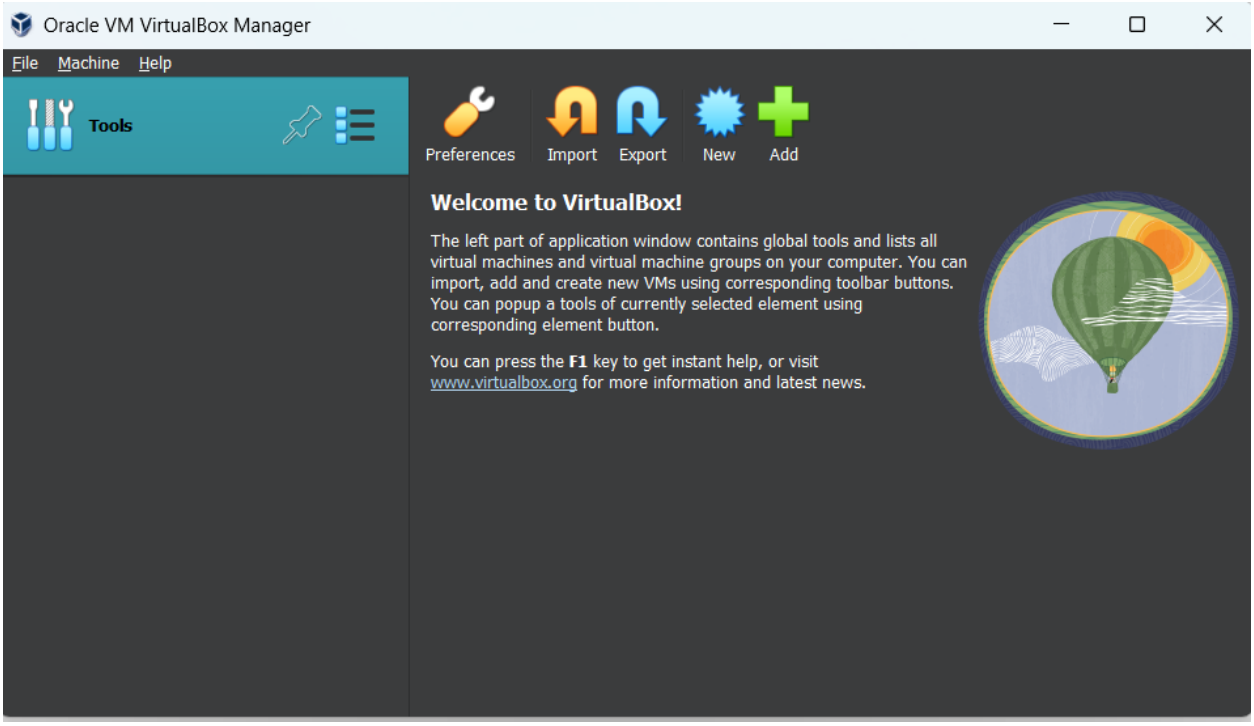


Step 5: Click on the install button.

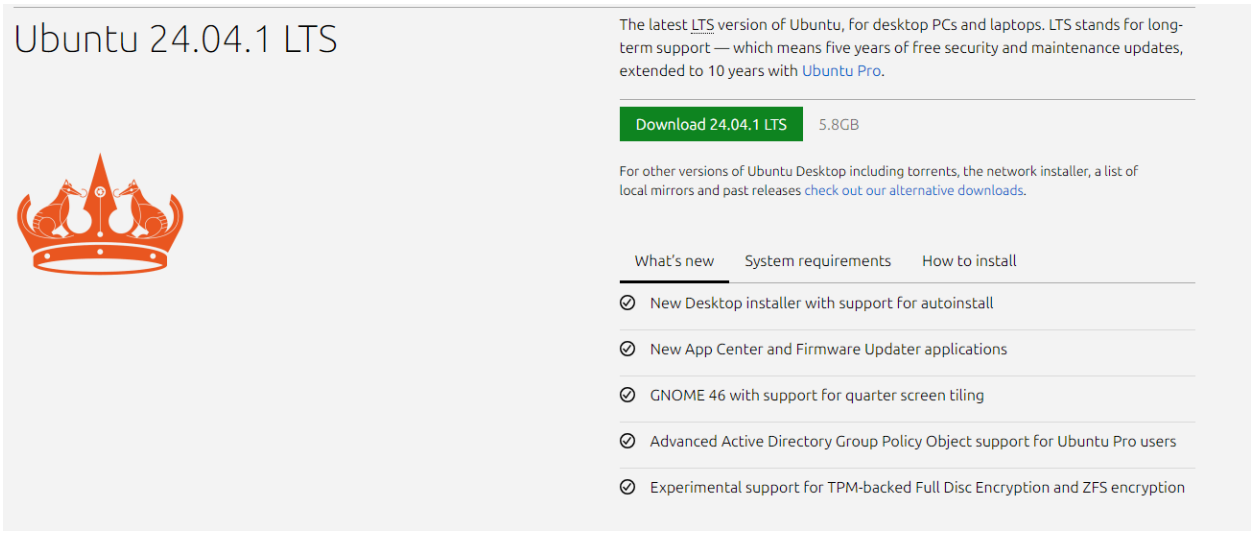


Step 6: After installation, click finish.

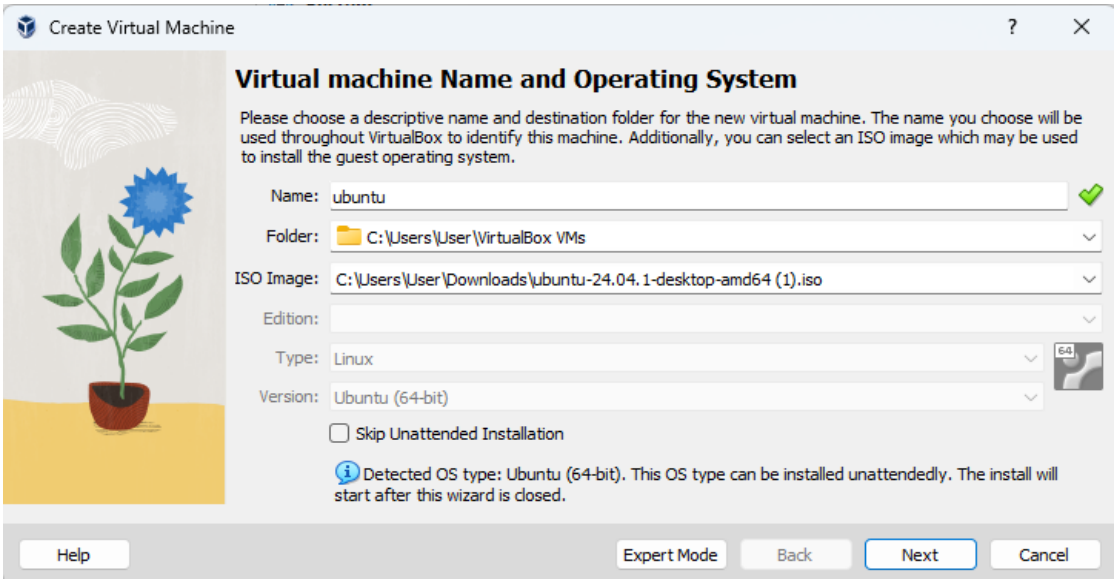
This is the first interface in the virtual box. Click on add to ubuntu as linux distribution.



This is official website to download ubuntu. https://ubuntu.com/download

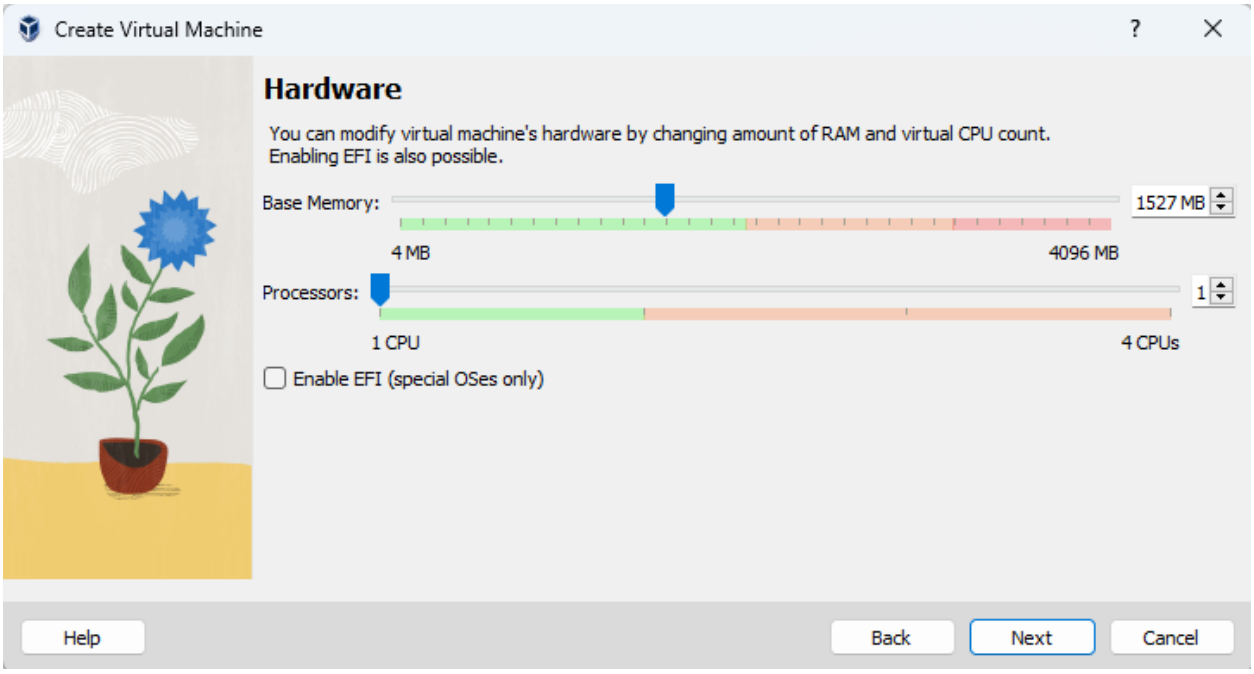


In this step name your virtual machine. Under, type select Linux and select ubuntu (64- bit) under version.

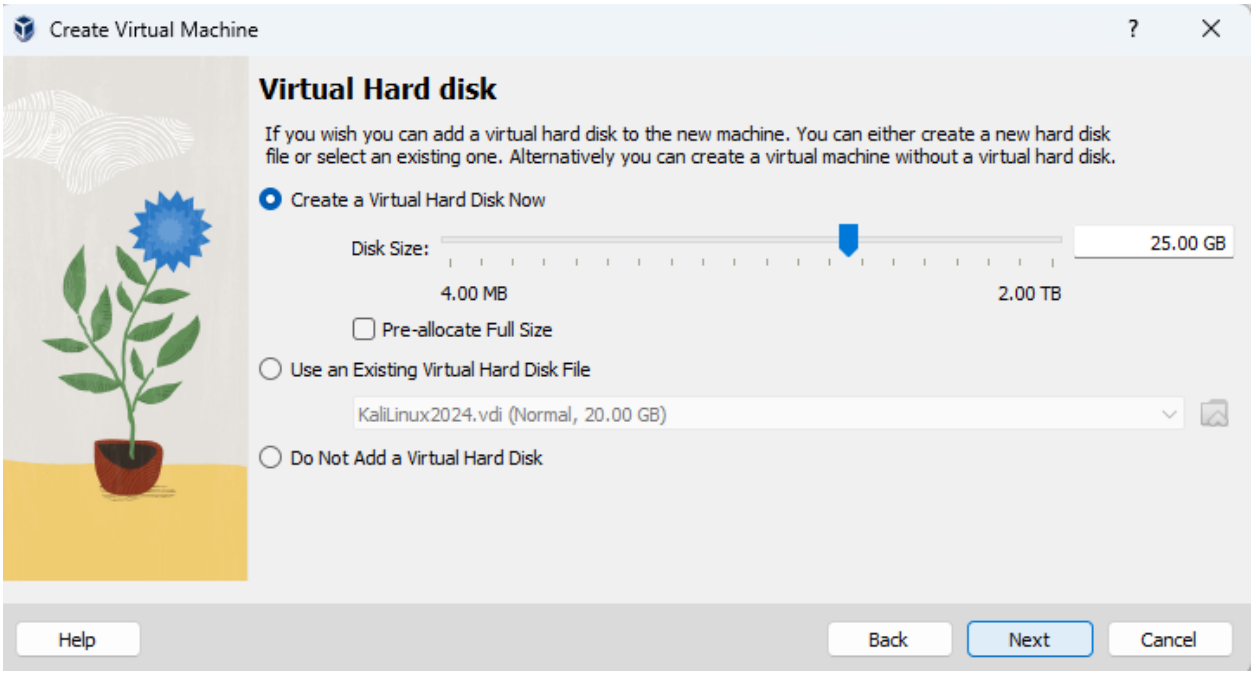


In this step add your new credentials to ubuntu virtual machine.

Choose the amount of memory (RAM) for virtual machine.

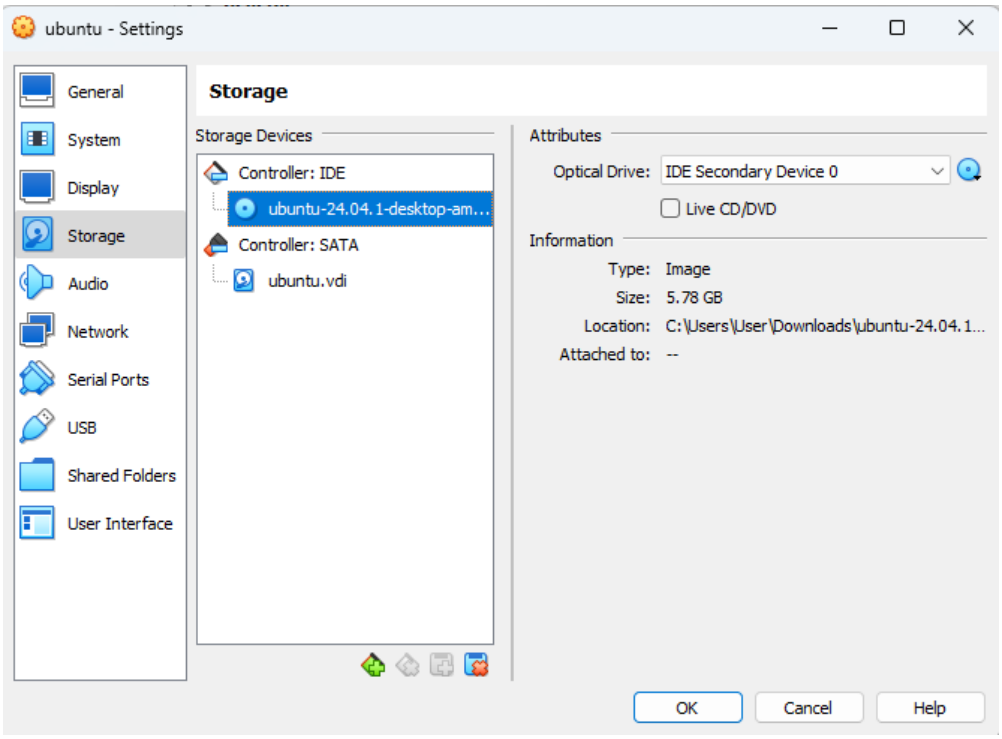


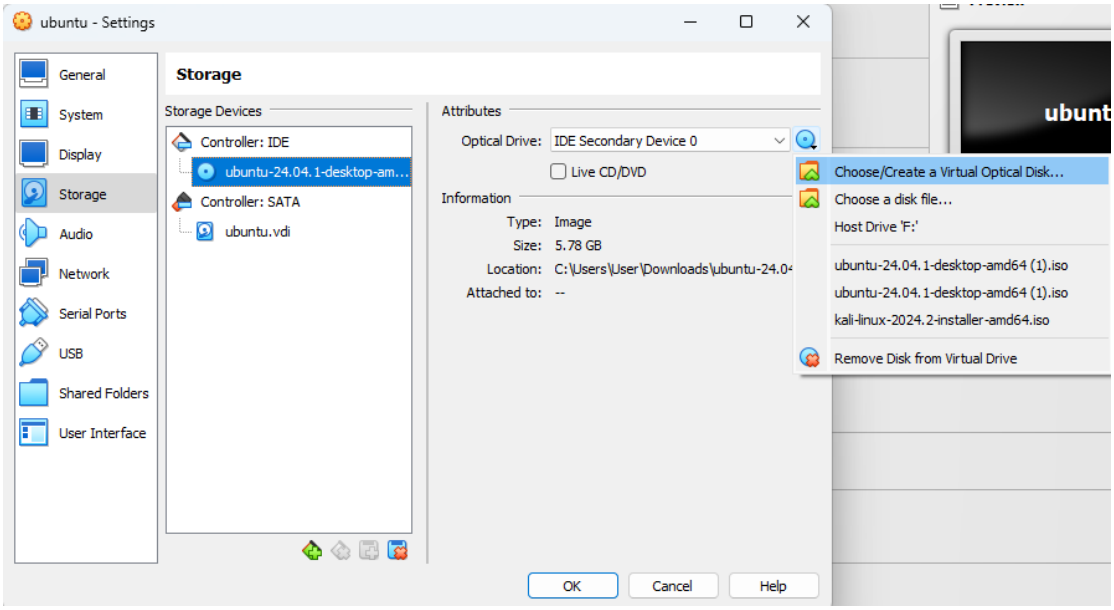
Set the virtual hard disk type.



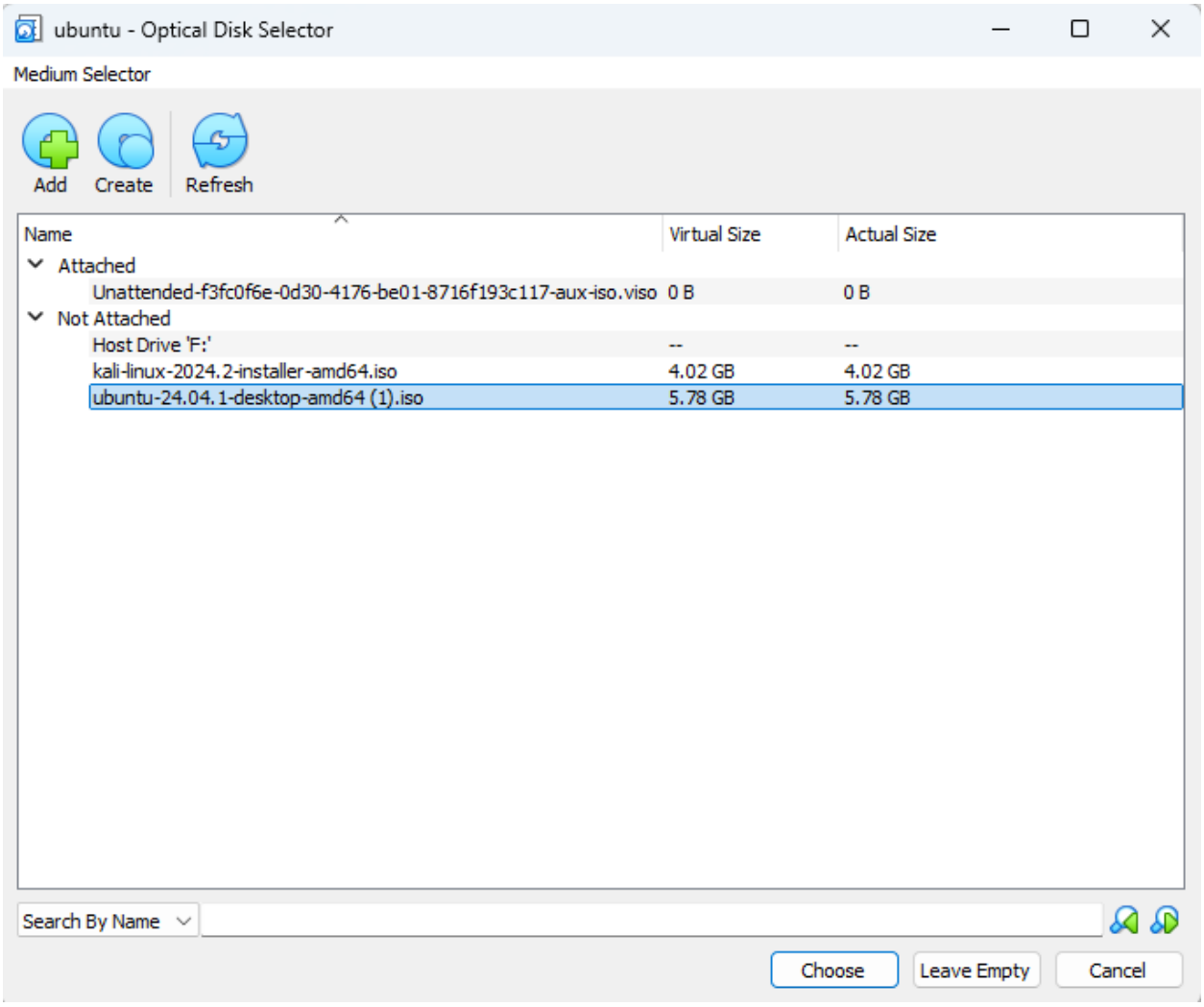
Select ubuntu virtual machine in the virtual box interface and click settings.

Go to the storage tab, under controller: IDE, click the empty disk icon and select choose a disk file.





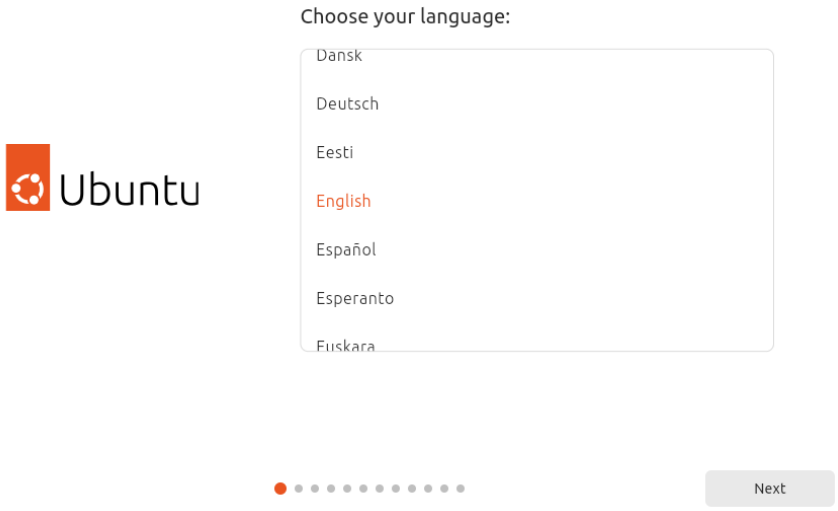
Browse to the ubuntu ISO that downloaded earlier and select it.

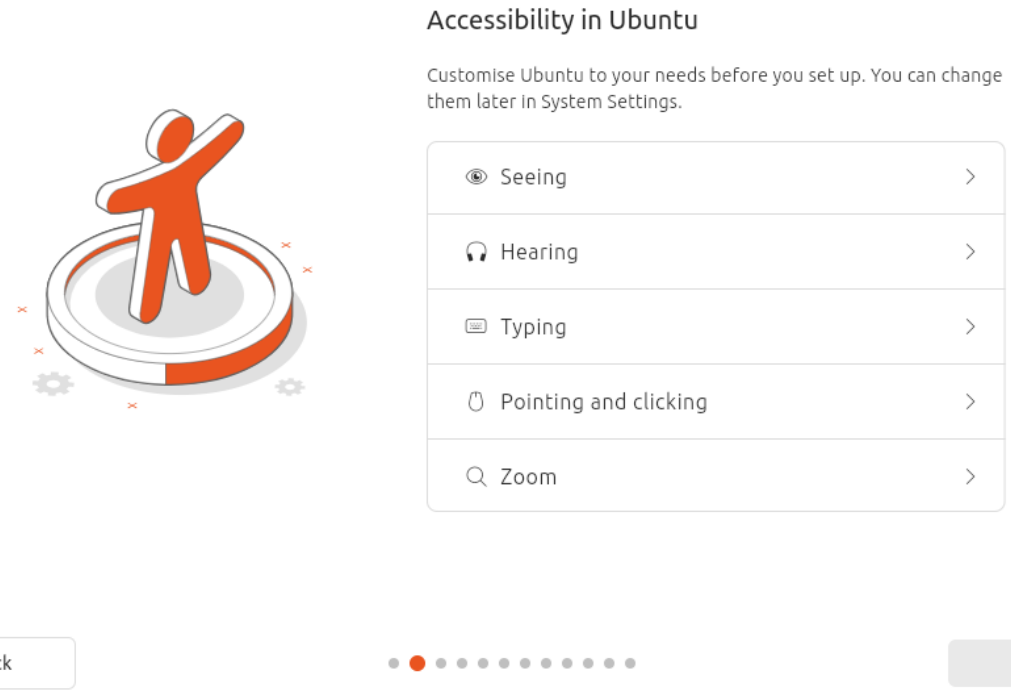


Click start to boot up the virtual machine. VirtualBox will boot from the ubuntu ISO. The ubuntu installer will load.

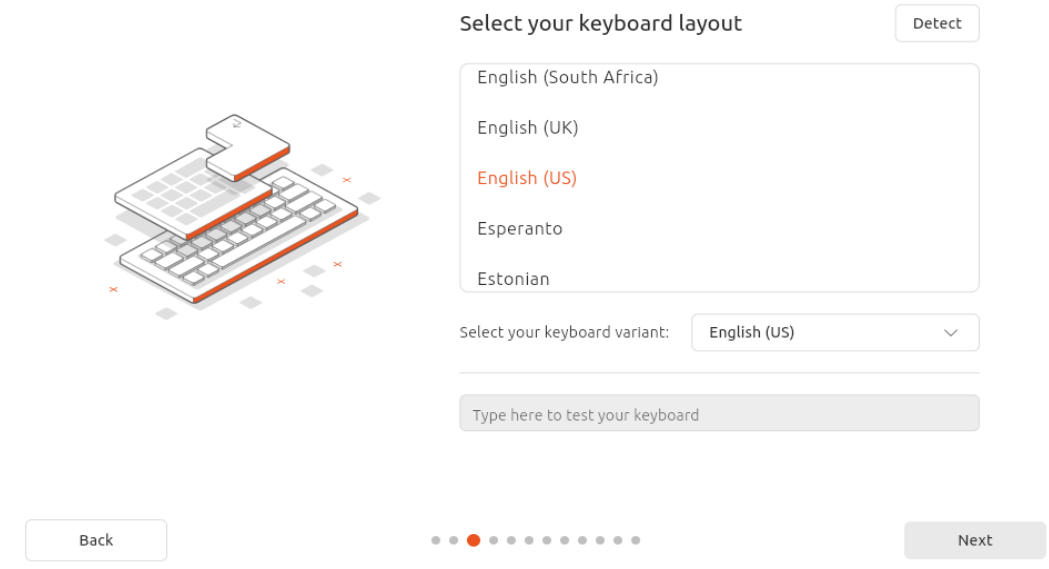
This is the ubuntu installation process.

Select the language.

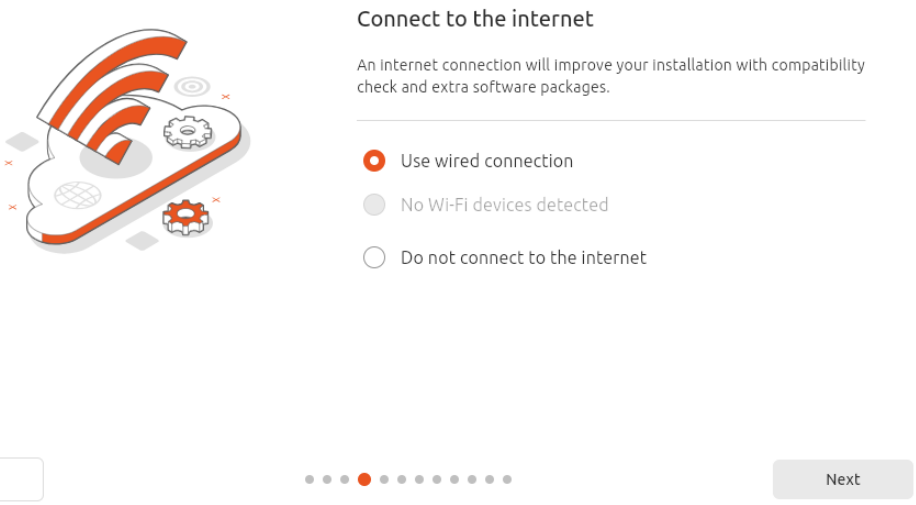




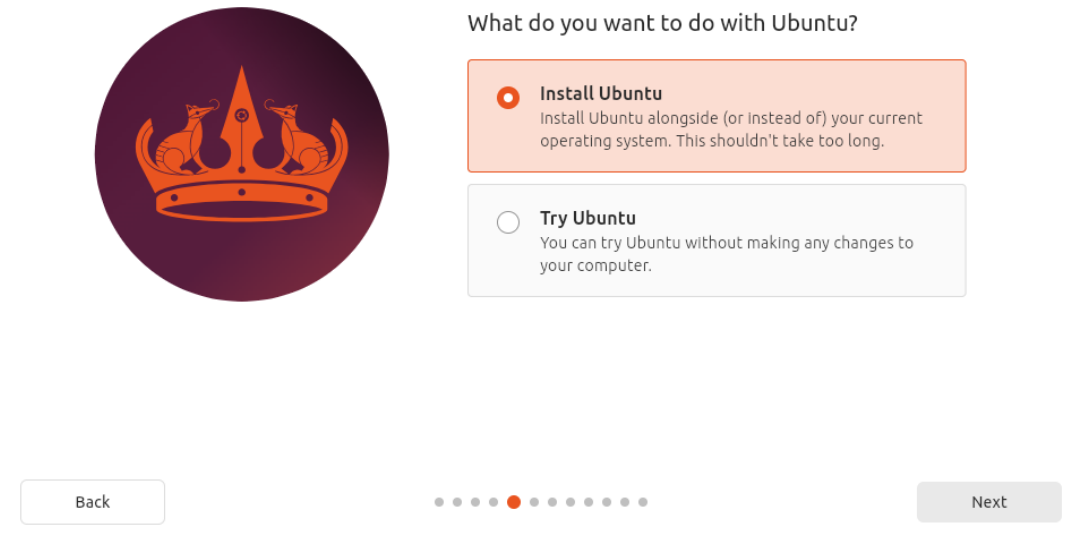
Select the keyboard layout.



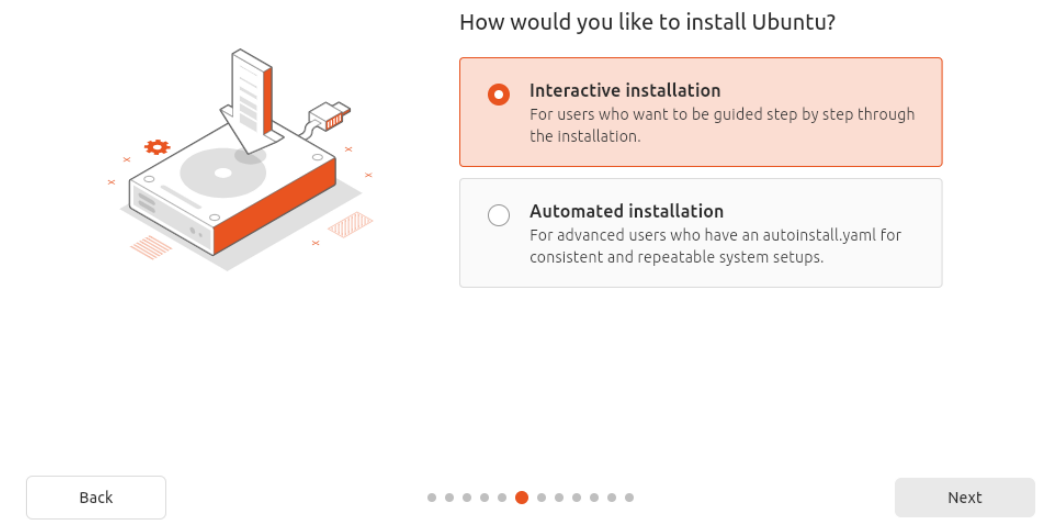
Select the network connection type. If you use wi-fi, only option is to select wired connection.



Choose the install ubuntu.



Choose interactive installation.



What apps would you like to install to start with?

Default selection
Just the essentials, web browser and basic utilities.

Extended selection
An offline-friendly selection of office tools, utilities and web browser.

Warning: The computer is not plugged in to a power source.

Back

Next

How do you want to install Ubuntu?

Erase disk and install Ubuntu
Start from scratch on your selected disk.

Advanced features... None selected

Manual installation
For advanced users seeking customized disk setups.

Back

Next

Install recommended proprietary software?

Ubuntu ships with no proprietary software by default. Installing additional software may improve your computer's performance.

- [x] Install third-party software for graphics and Wi-Fi hardware
  Including but not limited to NVIDIA drivers and similar
- [x] Download and install support for additional media formats
  Including but not limited to MP3, MP4, MOV and similar

Warning: The computer is not plugged in to a power source.

Back Next

Devices Help

Create your account

Your name: chanuli

Your computer's name: chanuli-VirtualBox

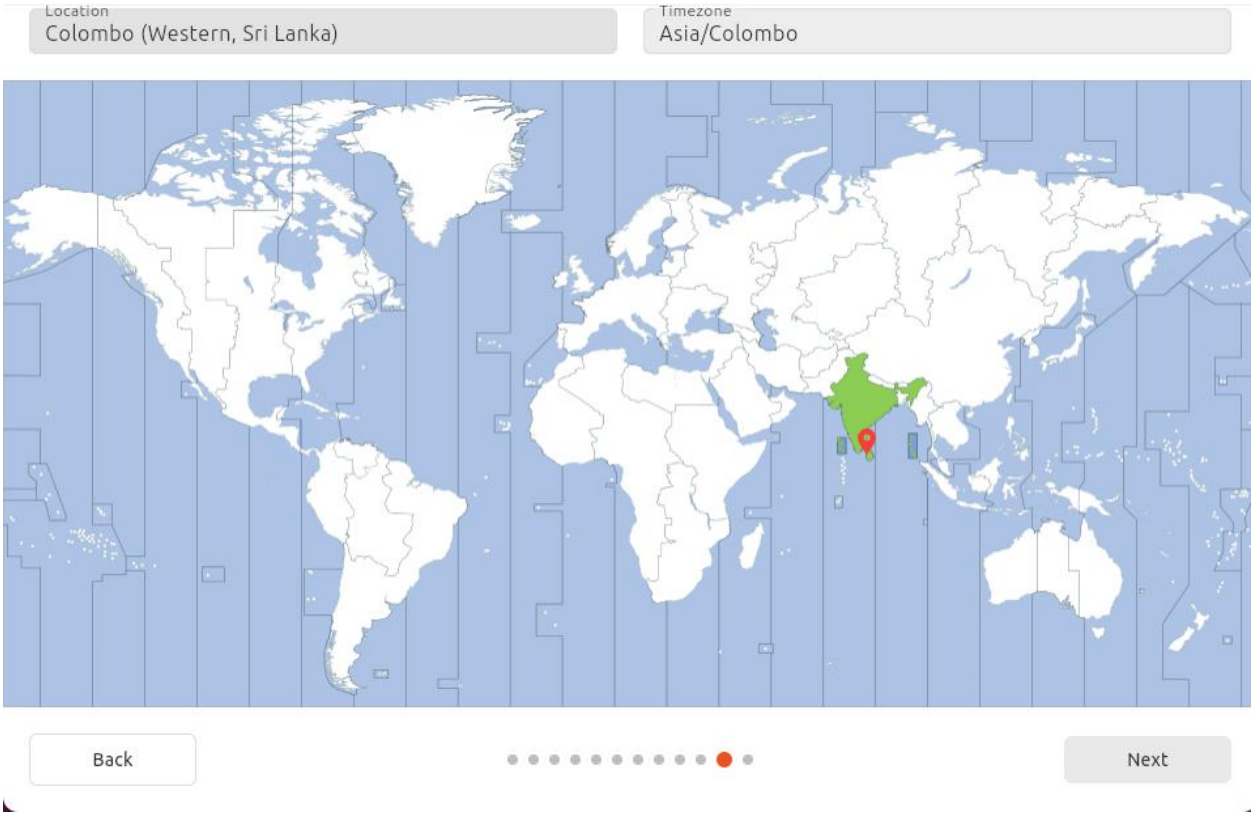
Your username: chanuli

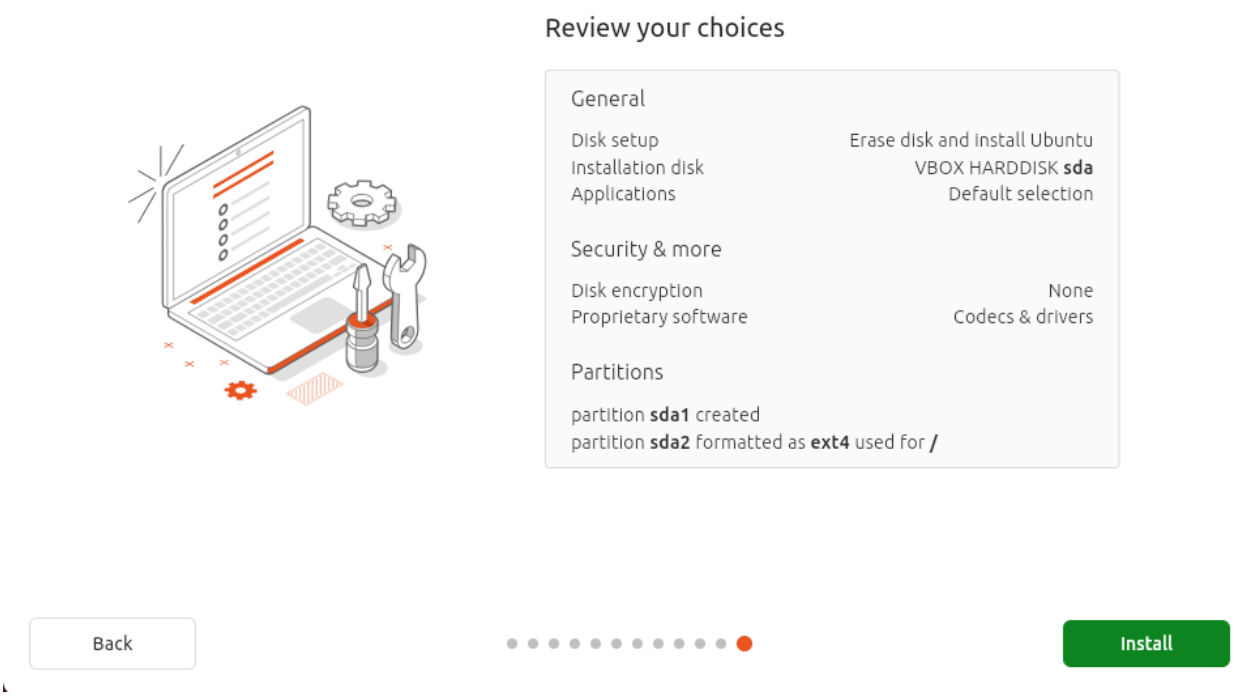
Password: •••••••••• Show Good password

Confirm password: ••••••••••

- [x] Require my password to log in
- [ ] Use Active Directory

Back Next


Location
Colombo (Western, Sri Lanka)
Timezone
Asia/Colombo
Back
Next


Review your choices
General
Disk setup
Erase disk and install Ubuntu
Installation disk
VBOX HARDDISK sda
Applications
Default selection
Security & more
Disk encryption
None
Proprietary software
Codecs & drivers
Partitions
partition sda1 created
partition sda2 formatted as ext4 used for /
Back
Install

Command Line Introduction

1.pwd - Command “pwd” print the name of the current working directory.

```
chanuli@chanuli-VirtualBox:~$ pwd
/home/chanuli
```

2.mkdir - Command “mkdir” create directory, if they do not already exist.

```
chanuli@chanuli-VirtualBox:~$ mkdir snp
```

3.rmdir - Command “rmdir” used to remove the directories if they are empty.

```
chanuli@chanuli-VirtualBox:~$ mkdir sos
chanuli@chanuli-VirtualBox:~$ ls
Desktop    Downloads  Pictures  snap  sos        Videos
Documents  Music      Public    snp   Templates
chanuli@chanuli-VirtualBox:~$ rmdir sos
chanuli@chanuli-VirtualBox:~$ ls
Desktop    Downloads  Pictures  snap  Templates
Documents  Music      Public    snp   Videos
```

4.ls - Command “ls” list information about the files(the current directory default).

```
chanuli@chanuli-VirtualBox:~$ ls
Desktop    Downloads  Pictures  snap  Templates
Documents  Music      Public    snp   Videos
```

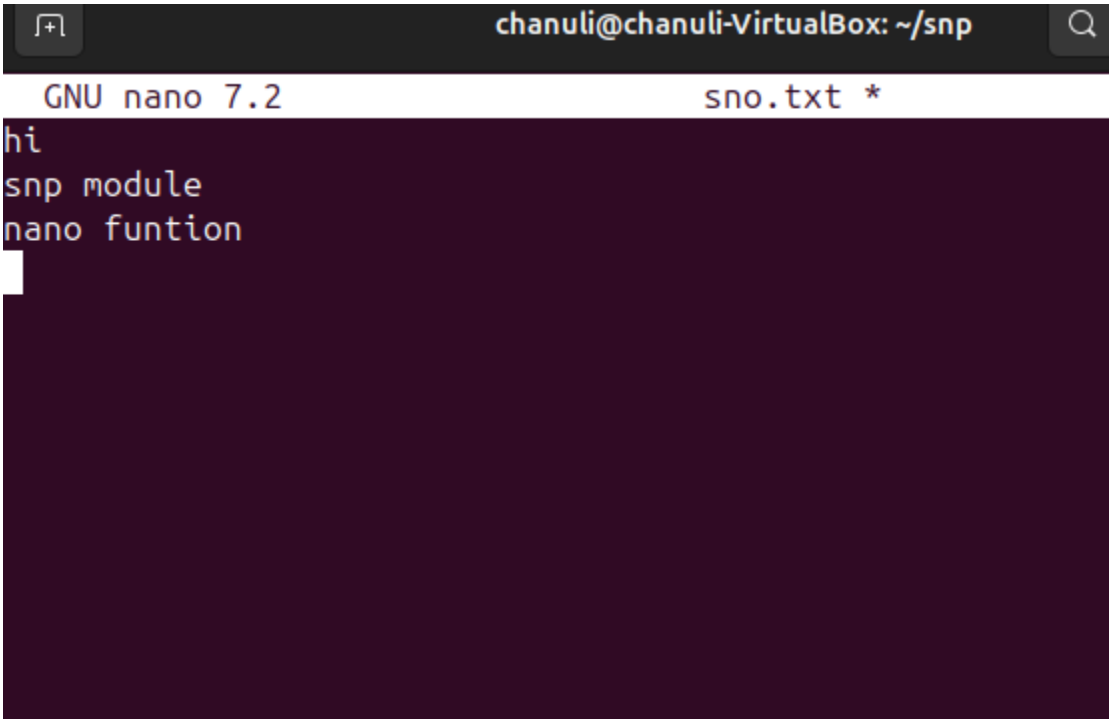
```
chanuli@chanuli-VirtualBox:~/snp$ ls -al
total 16
drwxrwxr-x  2 chanuli chanuli 4096 Sep 15 09:24 .
drwxr-x--- 16 chanuli chanuli 4096 Sep 15 09:14 ..
-rw-rw-r--  1 chanuli chanuli   28 Sep 15 09:24 snp1.txt
-rw-rw-r--  1 chanuli chanuli   28 Sep 15 09:18 snp.txt
```

5.cd - Command “cd” used to change the current working directory.

```
chanuli@server:~$ ls
backup   Documents  localhost.key  Pictures  snap  system_reports  Videos
Desktop  Downloads  Music          Public    snp   Templates
chanuli@server:~$ pwd
/home/chanuli
chanuli@server:~$ cd Desktop
chanuli@server:~/Desktop$ pwd
/home/chanuli/Desktop
```

6.nano - The nano is a small and friendly text editor. After nano you need to provide file name that you need to create or edit. After write you need to press ctrl+o and enter. After by pressing ctrl+x you can save and exit from file.

```
chanuli@chanuli-VirtualBox:~/snp$ nano sno.txt
```



7.cat - Command “cat” used to concatenate files and print on the standard output.

```
chanuli@chanuli-VirtualBox:~/snp$ cat sno.txt
hi
snp module
nano funtion
```

8.mv - Command “mv” used to rename source file to destination file or move source to directory.

The syntax is source_file destination_file.

```
chanuli@chanuli-VirtualBox:~/snp$ mv sno.txt snp.txt
chanuli@chanuli-VirtualBox:~/snp$ ls
snp.txt
```

9.cp - Command “cp” used to copy files and directory.

cp source_file_name new_file_name

```
chanuli@chanuli-VirtualBox:~/snp$ cp snp.txt snp1.txt
chanuli@chanuli-VirtualBox:~/snp$ ls
snp1.txt  snp.txt
```

10.chmod - Command “chmod” used to change file mode bit (change file permission). It can be change in two ways either symbolic representation or octal representation.

- r – read permission
- w – write permission
- x – execute permission

```
chanuli@chanuli-VirtualBox:~/snp$ ls -al
total 16
drwxrwxr-x  2 chanuli chanuli 4096 Sep 15 09:24 .
drwxr-x--- 16 chanuli chanuli 4096 Sep 15 09:14 ..
-rw-rw-r--  1 chanuli chanuli   28 Sep 15 09:24 snp1.txt
-rw-rw-r--  1 chanuli chanuli   28 Sep 15 09:18 snp.txt
```

```
chanuli@chanuli-VirtualBox:~/snp$ chmod +x snp.txt
chanuli@chanuli-VirtualBox:~/snp$ ls -al
total 16
drwxrwxr-x  2 chanuli chanuli 4096 Sep 15 09:24 .
drwxr-x--- 16 chanuli chanuli 4096 Sep 15 09:14 ..
-rw-rw-r--  1 chanuli chanuli   28 Sep 15 09:24 snp1.txt
-rwxrwxr-x  1 chanuli chanuli   28 Sep 15 09:18 snp.txt
```

11.rm - Command “rm” used to remove each specified file

```
chanuli@chanuli-VirtualBox:~/snp$ ls
snp1.txt  snp.txt
```

```
chanuli@chanuli-VirtualBox:~/snp$ rm snp.txt
chanuli@chanuli-VirtualBox:~/snp$ ls
snp1.txt
```

12. grep - Command “grep” is used to search for pattens in each file. Patterns is one or more patterns separated by new line characters and grep print each line that matches a pattern.

```
chanuli@chanuli-VirtualBox:~/snp$ grep snp snp1.txt
snp module
```

13. head/tail - Command “head” print the first ten lines of each file to standard output and “tail” print the last ten lines of each file to standard output.

```
chanuli@chanuli-VirtualBox:~/snp$ head snp1.txt
hi
snp module
nano funtion
head
tail
function testing
commands
semester
Y2S1
Modules
chanuli@chanuli-VirtualBox:~/snp$ tail snp1.txt
function testing
commands
semester
Y2S1
Modules
SNP
DBMS
SOS
ICS
```

System Information and User Management

14. uname - Command “uname” print system information. Flag “-a” used to print all information like kernel name, network node hostname, kernel release, kernel version, machine hardware name.

- Kernel name – Linux
- Hostname – server.example.com
- Kernel version – 6.8.0-45-generic
- Machine type - x86_64

```
chanuli@server:~$ uname -a
Linux server.example.com 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug
 30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
```

15. Command “cat /proc/version” used to display the Linux kernel version and GNU compiler version used to build it. The “proc” file system is a pseudo-filesystem which provides an interface to kernel data structures.

```
chanuli@server:~$ cat /proc/version
Linux version 6.8.0-45-generic (buildd@lcy02-amd64-115) (x86_64-linux-gnu-gcc-13 (Ubuntu 1
3.2.0-23ubuntu4) 13.2.0, GNU ld (GNU Binutils for Ubuntu) 2.42) #45-Ubuntu SMP PREEMPT_DYN
AMIC Fri Aug 30 12:02:04 UTC 2024
```

16. df - Command “df” display the amount of the space available on the file system containing each file name argument. Flag “-h” used to print sizes in power of 1024 as human readable way.

```
chanuli@server:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           795M  1.5M  793M   1% /run
/dev/sda2        25G   11G   13G  48% /
tmpfs           3.9G     0  3.9G   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           795M  136K  795M   1% /run/user/1000
/dev/sr0         52M   52M     0 100% /media/chanuli/VBox_GAs_7.0.20
```

17. id - Command “id” print user and group information for each specified user or current process(when user omitted)

```
chanuli@server:~$ id
uid=1000(chanuli) gid=1000(chanuli) groups=1000(chanuli),4(adm),24(cdrom),27(sudo),30(dip)
,46(plugdev),100(users),114(lpadmin)
```

18. free - Command “free” used to display the total amount of free and used physical and swap memory in the system, as well as the buffers and caches used by the kernal. Flag “-m” used to show output in mebibytes.

```
chanuli@server:~$ free
               total        used        free      shared  buff/cache   available
Mem:         8132720     1227100     6334024       32744      843144     6905620
Swap:        4194300           0     4194300
chanuli@server:~$ free -m
               total        used        free      shared  buff/cache   available
Mem:            7942        1198        6185          31         823        6743
Swap:           4095           0        4095
```

19. whoami - Command “whoami” print effective user name. this command is useful for verifying which user is currently log in.

```
chanuli@server:~$ whoami
chanuli
```

20. passwd - Command “passwd” changes passwords for user accounts. A normal user may only change the password for their own account, while the superuser may change the password for any account.

```
chanuli@server:~$ passwd
Changing password for chanuli.
Current password:
```

21. useradd - Command “useradd” used to create a new user or update default new user information.

```
chanuli@server:~$ sudo useradd ubuntu
```

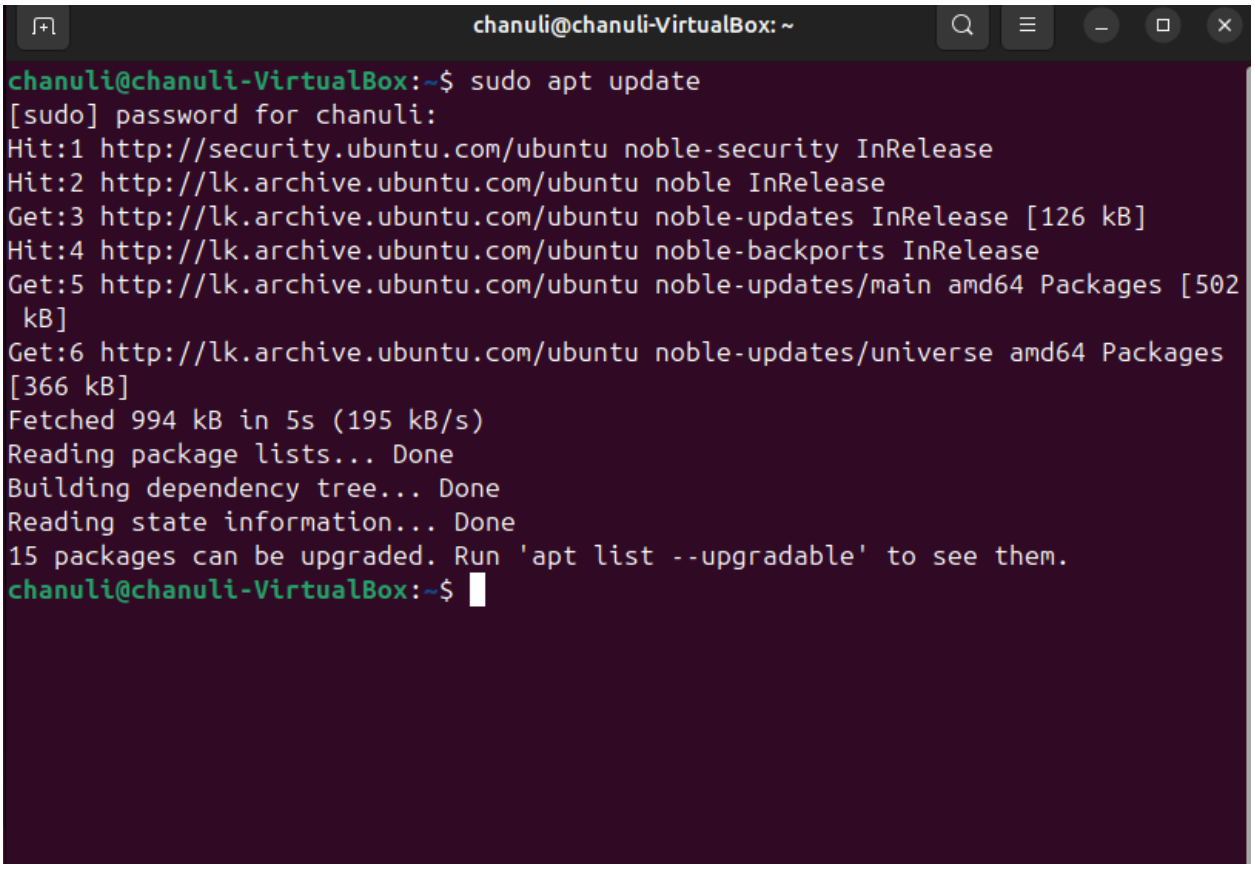
2.DHCP, DNS and NTP Services

DHCP (Dynamic Host Configuration Protocols)

Dynamic Host Configuration Protocol is a network management protocol that we use on TCP/IP network. The DHCP server, automatically assigns IP addresses and other network configurations like subnet mask, default gateway, DNS server and more to the connected devices so they can exchange information.

1. Install the DHCP server
   - First update the package list to ensure that we are downloading the latest version.

Update package list - sudo apt update



- Then install the DHCP server.

sudo apt install isc-dhcp-server – This command installs the isc-dhcp-server, which is the most common dhcp server for linux.

```
chanuli@chanuli-VirtualBox:~$ sudo apt install isc-dhcp-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  isc-dhcp-common
Suggested packages:
  isc-dhcp-server-ldap policycoreutils
The following NEW packages will be installed:
  isc-dhcp-common isc-dhcp-server
0 upgraded, 2 newly installed, 0 to remove and 15 not upgraded.
Need to get 1,281 kB of archives.
After this operation, 4,281 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-server amd64 4.4.3-P1-4ubuntu2 [1,236 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-common amd64 4.4.3-P1-4ubuntu2 [45.8 kB]
Fetched 1,281 kB in 5s (282 kB/s)
Preconfiguring packages ...
Selecting previously unselected package isc-dhcp-server.
(Reading database ... 151099 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-server_4.4.3-P1-4ubuntu2_amd64.deb ...
```

2. Configure the DHCP server

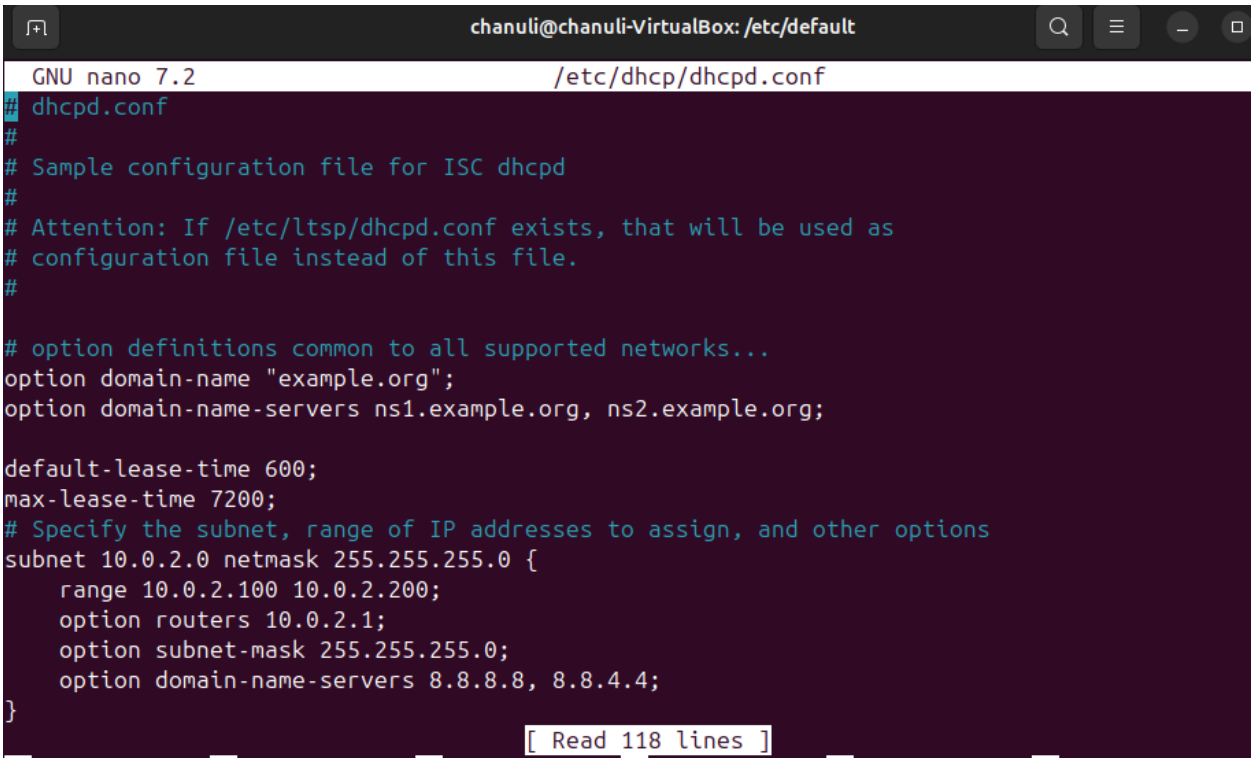
- Edit the DHCP configuration file- This file defines how the DHCP server operates and how it assigns ip addresses.

```
chanuli@chanuli-VirtualBox:~$ cd /etc/dhcp
chanuli@chanuli-VirtualBox:/etc/dhcp$ ls
ddns-keys  dhclient-exit-hooks.d  dhcpd6.conf  dhcpd.conf
```

```
chanuli@chanuli-VirtualBox:/etc/default$ sudo nano /etc/dhcp/dhcpd.conf
```

- subnet 10.0.2.0 – This represents the starting point of the subnet and is not assignable to any devices. It indicates that the server will operate within this network.
- Netmask is a 32-bit number that divides an ip address into the network and host portions. It defines the range of ip address that belongs to a specific subnet.

- range 10.0.2.100 10.0.2.200 – This means that any client requesting an ip address will be assigned an address in this range. This configuration allows the dhcp server to dynamically assign ip address to devices connected to the networks.
- option subnet-mask 255.255.255.0 – This specifies the subnet mask for the clients receiving ip addresses from the DHCP server.
- option routers 10.0.2.1 – This specifies the default gateway foe clients on this subnet.
- option broadcast-address 10.0.2.255 – The broadcast address is used to communicate with all devices on the subnet simultaneously.
- default-lease-time 600 – lease is the amount of the time an ip address is assigned to a device. The DHCP server assign an ip address to a client for a default duration of 600 seconds (10 min). after this time the client must renew the lease
- max-lease-time 7200 – The maximum time a client can hold onto an ip address is set to two hours. If the client does not renew the lease within this time, it will have to request a new ip address from the DHCP server.



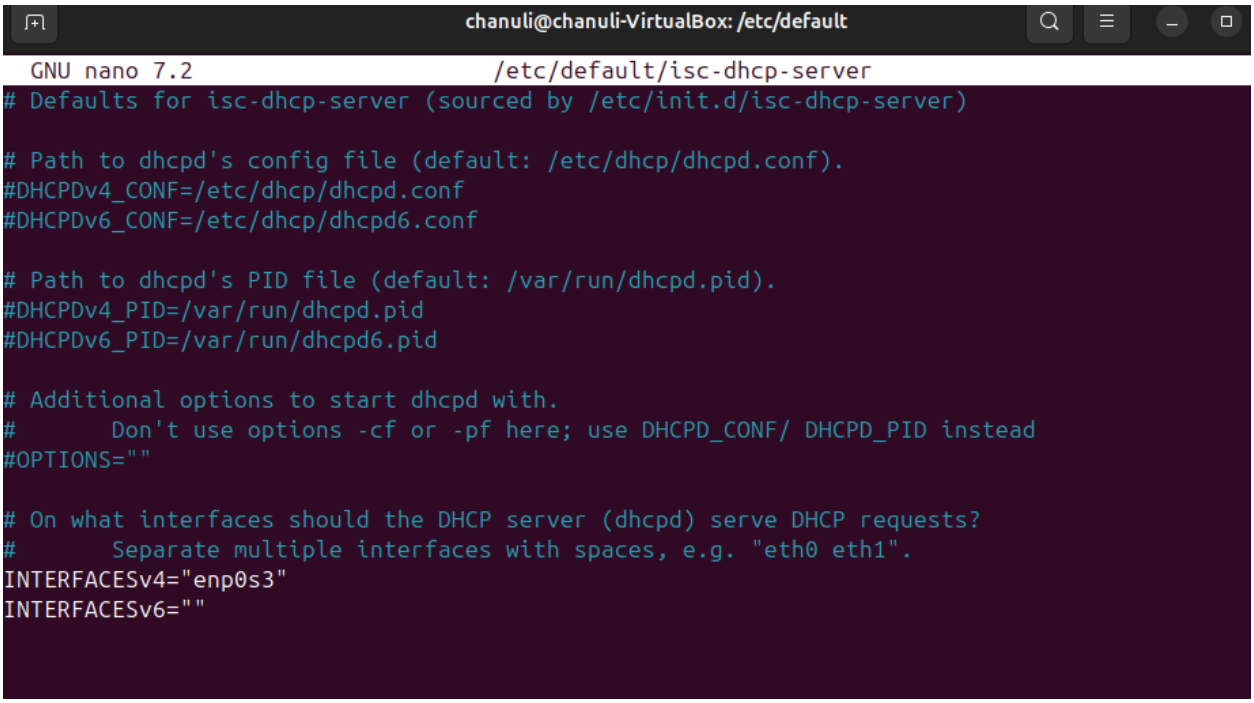
3. Specify the network interface
    - Edit the default file for DHCP – isc-dhcp-server is the file specifies which network interface DHCP should use listen for requests from clients.

```
chanuli@chanuli-VirtualBox:~$ cd /etc/dhcp
chanuli@chanuli-VirtualBox:/etc/dhcp$ cd /etc/default
chanuli@chanuli-VirtualBox:/etc/default$ ls
alsa              cron              isc-dhcp-server      rsync
amd64-microcode   dbus              kerneloops           saned
anacron           grub              keyboard             sssd
apport            grub.d            locale               sysstat
bluetooth         im-config         networkd-dispatcher  ufw
console-setup     intel-microcode   openvpn              useradd
```

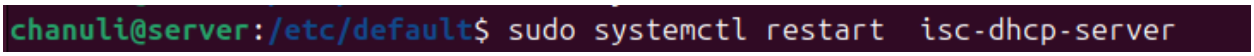
```
chanuli@chanuli-VirtualBox:/etc/default$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default q
len 1000
    link/ether 08:00:27:90:55:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 81277sec preferred_lft 81277sec
    inet6 fe80::a00:27ff:fe90:5555/64 scope link
       valid_lft forever preferred_lft forever
```

    - Set the interface variable – replace enp0s3 which the name of active network interface.

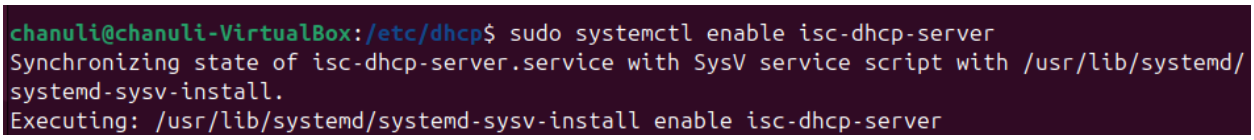
```
chanuli@server:/etc/default$ sudo nano isc-dhcp-server
[sudo] password for chanuli:
```



sudo systemctl restart isc-dhcp-server – this command restart the dhcp server applying any changes made to the configuration files.

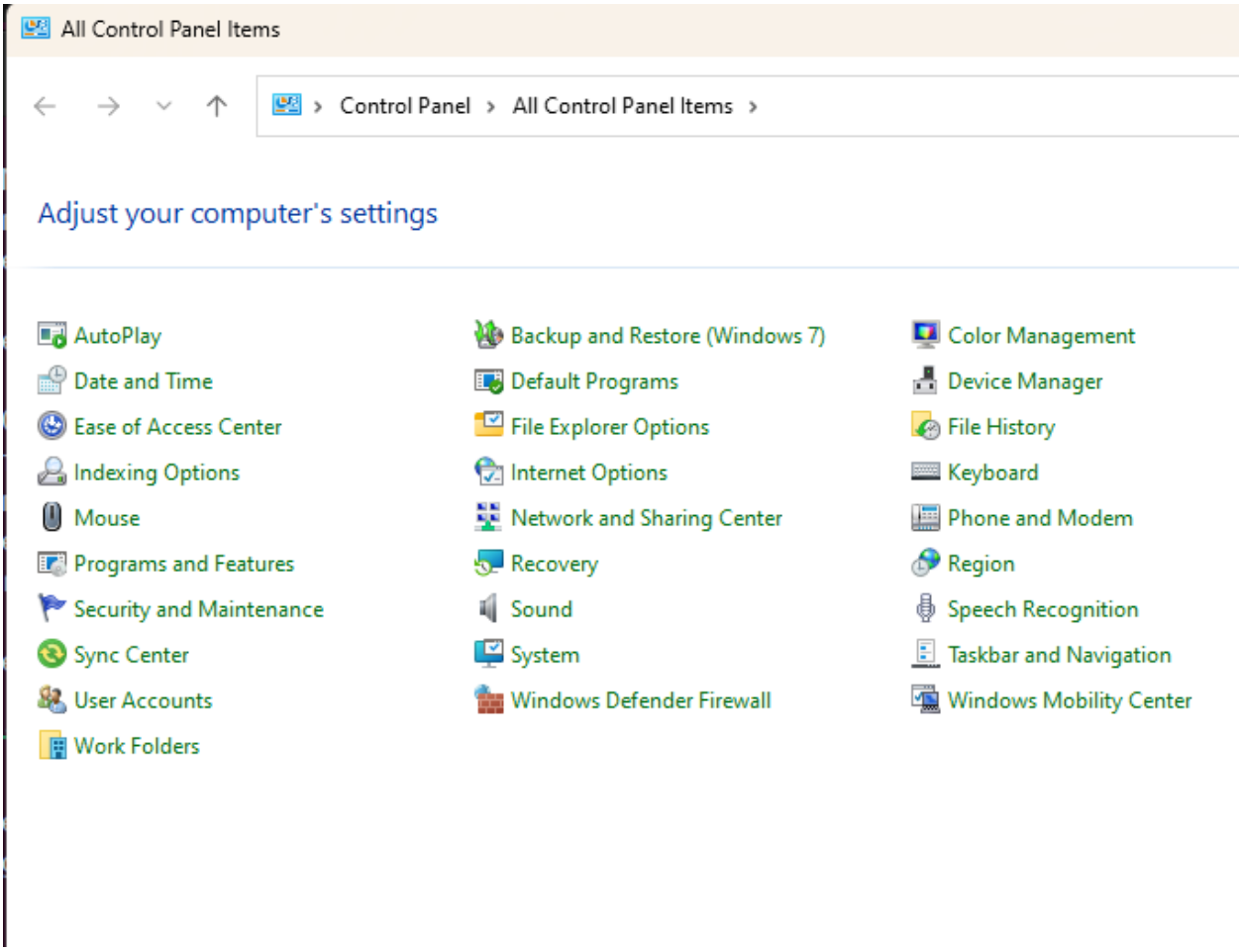


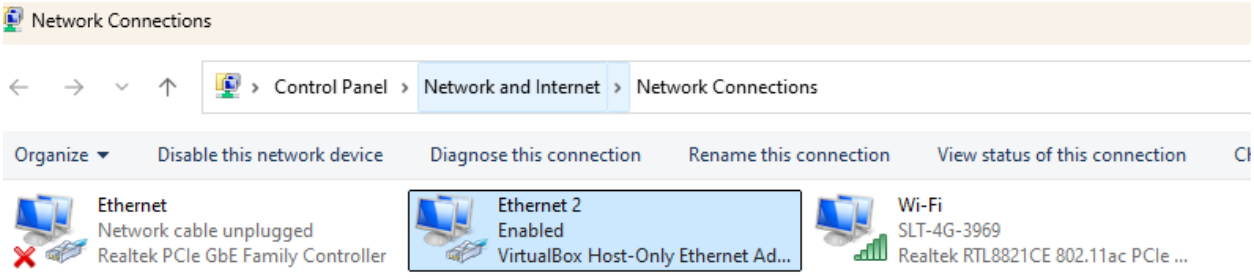
Enable service to start on boot.

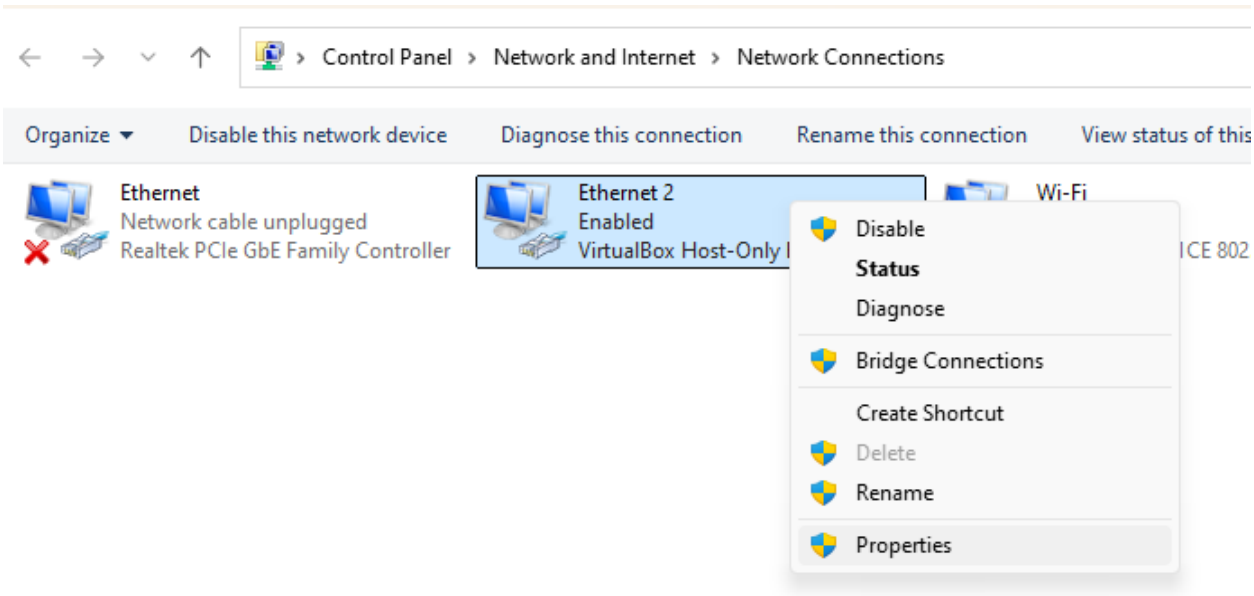


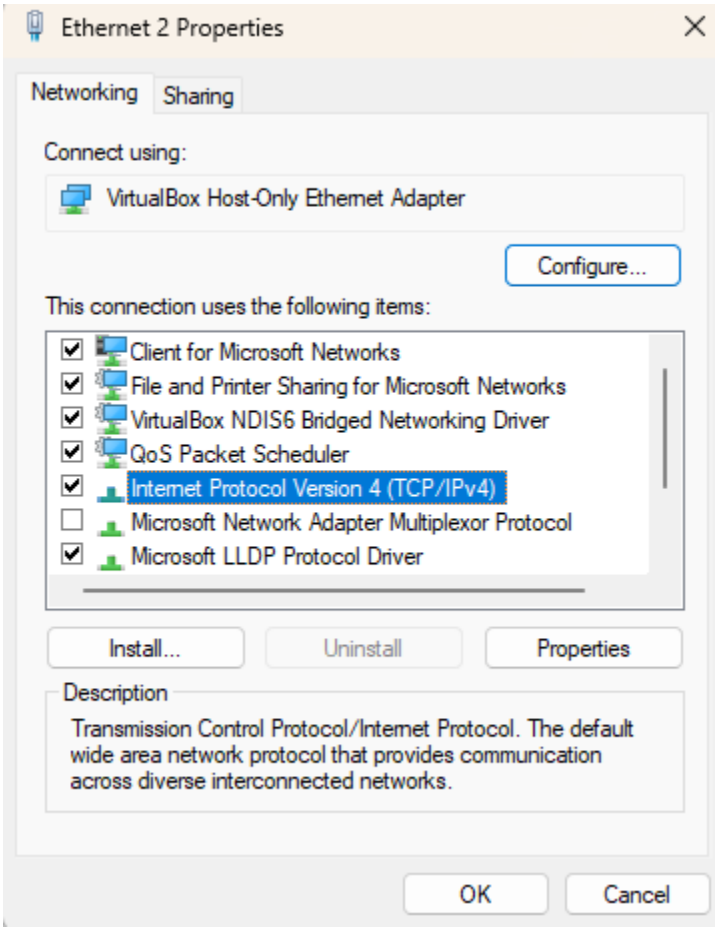
```
chanuli@chanuli-VirtualBox:/etc/default$ sudo systemctl restart isc-dhcp-server
chanuli@chanuli-VirtualBox:/etc/default$ systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-09-18 12:52:35 +0530; 23s ago
       Docs: man:dhcpd(8)
   Main PID: 4489 (dhcpd)
      Tasks: 1 (limit: 9446)
     Memory: 3.7M (peak: 4.0M)
        CPU: 17ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─4489 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /e>

Sep 18 12:52:35 chanuli-VirtualBox dhcpd[4489]: PID file: /run/dhcp-server/dhcpd.pid
Sep 18 12:52:35 chanuli-VirtualBox dhcpd[4489]: Wrote 0 leases to leases file.
Sep 18 12:52:35 chanuli-VirtualBox sh[4489]: Wrote 0 leases to leases file.
Sep 18 12:52:35 chanuli-VirtualBox dhcpd[4489]: Listening on LPF/enp0s3/08:00:27:90:55:55/10.0>
Sep 18 12:52:35 chanuli-VirtualBox sh[4489]: Listening on LPF/enp0s3/08:00:27:90:55:55/10.0.2.>
Sep 18 12:52:35 chanuli-VirtualBox sh[4489]: Sending on   LPF/enp0s3/08:00:27:90:55:55/10.0.2.>
Sep 18 12:52:35 chanuli-VirtualBox sh[4489]: Sending on   Socket/fallback/fallback-net
Sep 18 12:52:35 chanuli-VirtualBox dhcpd[4489]: Sending on   LPF/enp0s3/08:00:27:90:55:55/10.0>
Sep 18 12:52:35 chanuli-VirtualBox dhcpd[4489]: Sending on   Socket/fallback/fallback-net
Sep 18 12:52:35 chanuli-VirtualBox dhcpd[4489]: Server starting service.
```

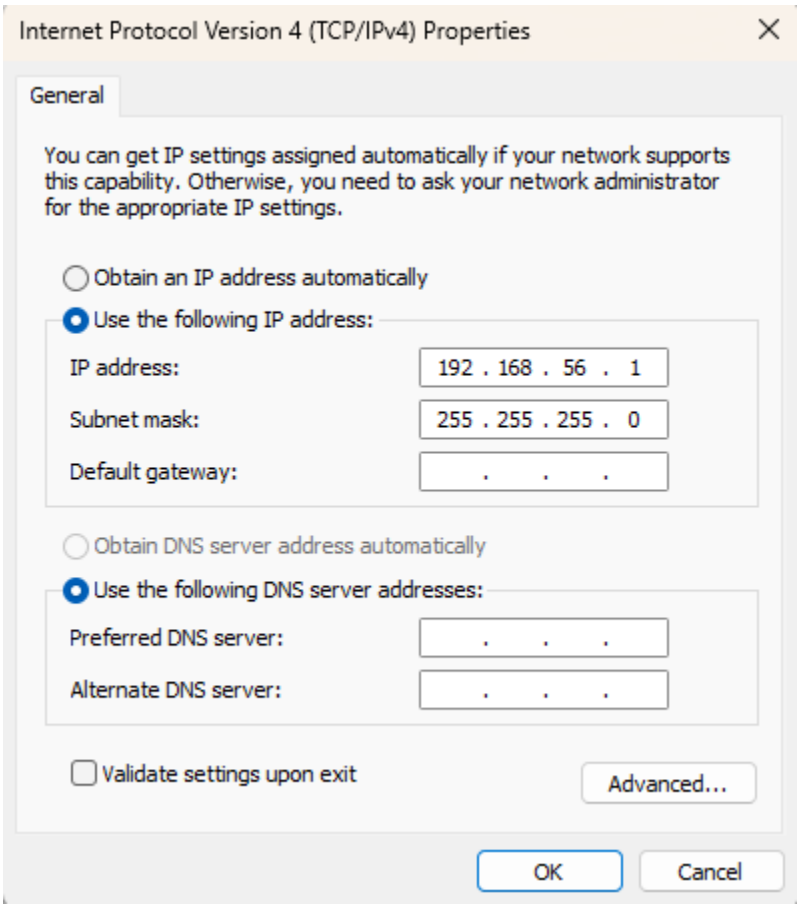
Verification

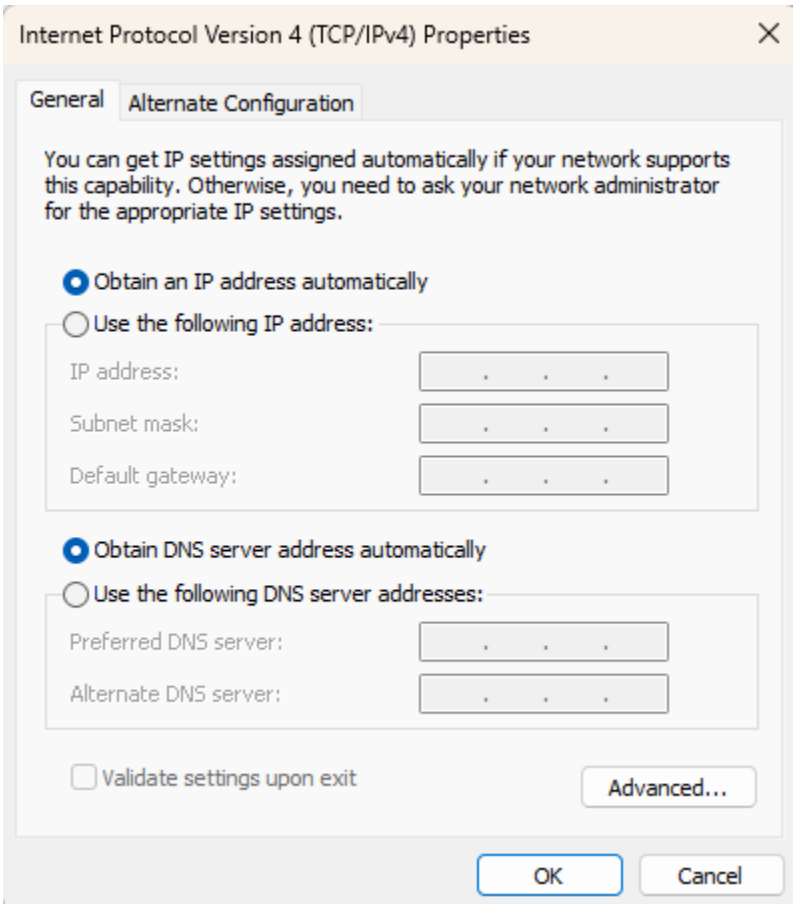





Control Panel › Network and Internet › Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this
Ethernet
Network cable unplugged
Realtek PCIe GbE Family Controller
Ethernet 2
Enabled
VirtualBox Host-Only
Wi-Fi
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties


Ethernet 2 Properties
Networking
Sharing
Connect using:
VirtualBox Host-Only Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
VirtualBox NDIS6 Bridged Networking Driver
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 56 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel




```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 84-A9-3E-A4-FE-82
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-04
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::956d:f6eb:e097:c0f8%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, October 1, 2024 8:26:29 AM
   Lease Expires . . . . . . . . . . : Tuesday, October 1, 2024 8:41:28 AM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.56.100
   DHCPv6 IAID . . . . . . . . . . . : 688521255
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-15-F5-D7-84-A9-3E-A4-FE-82
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

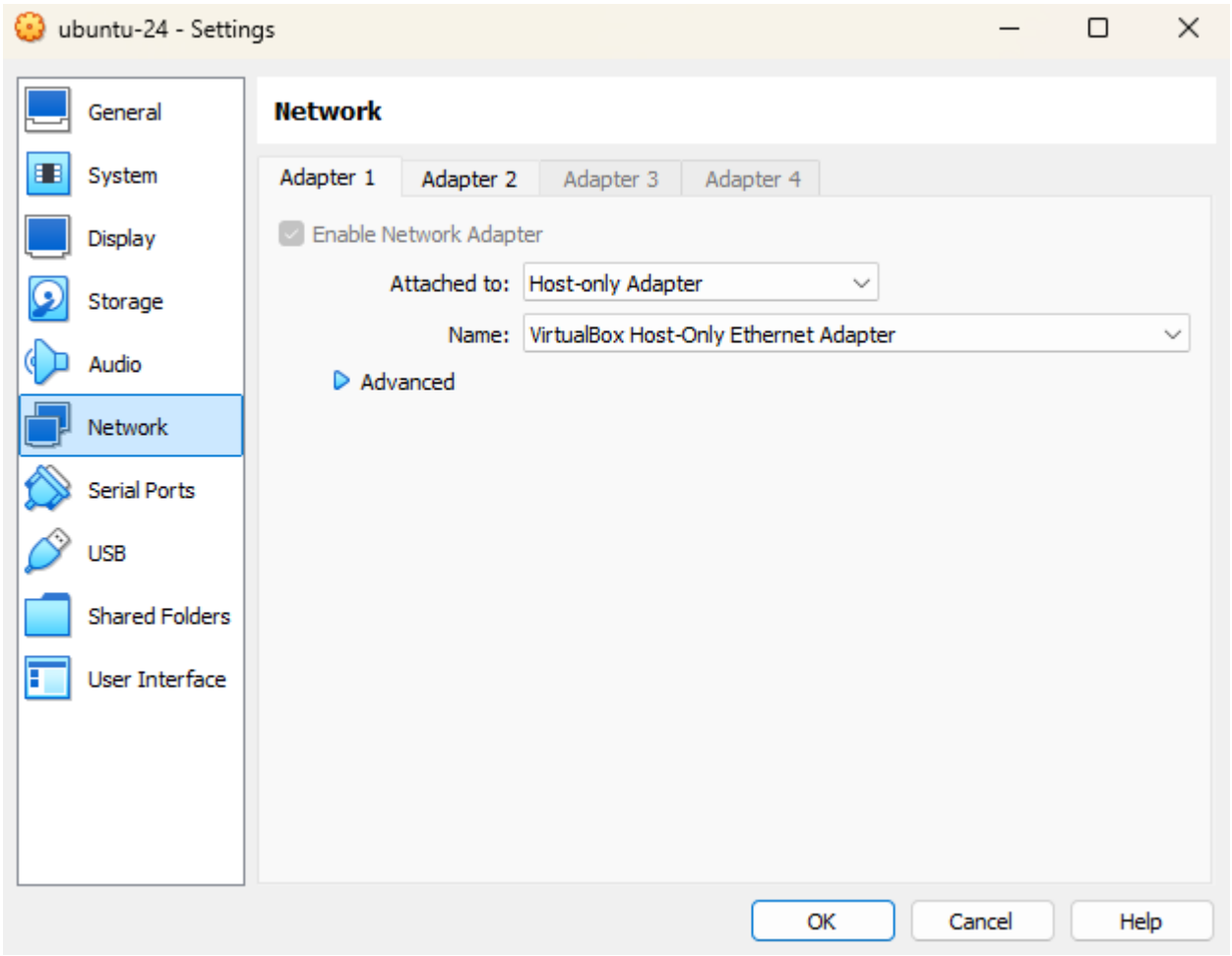
Install dhcp client version.

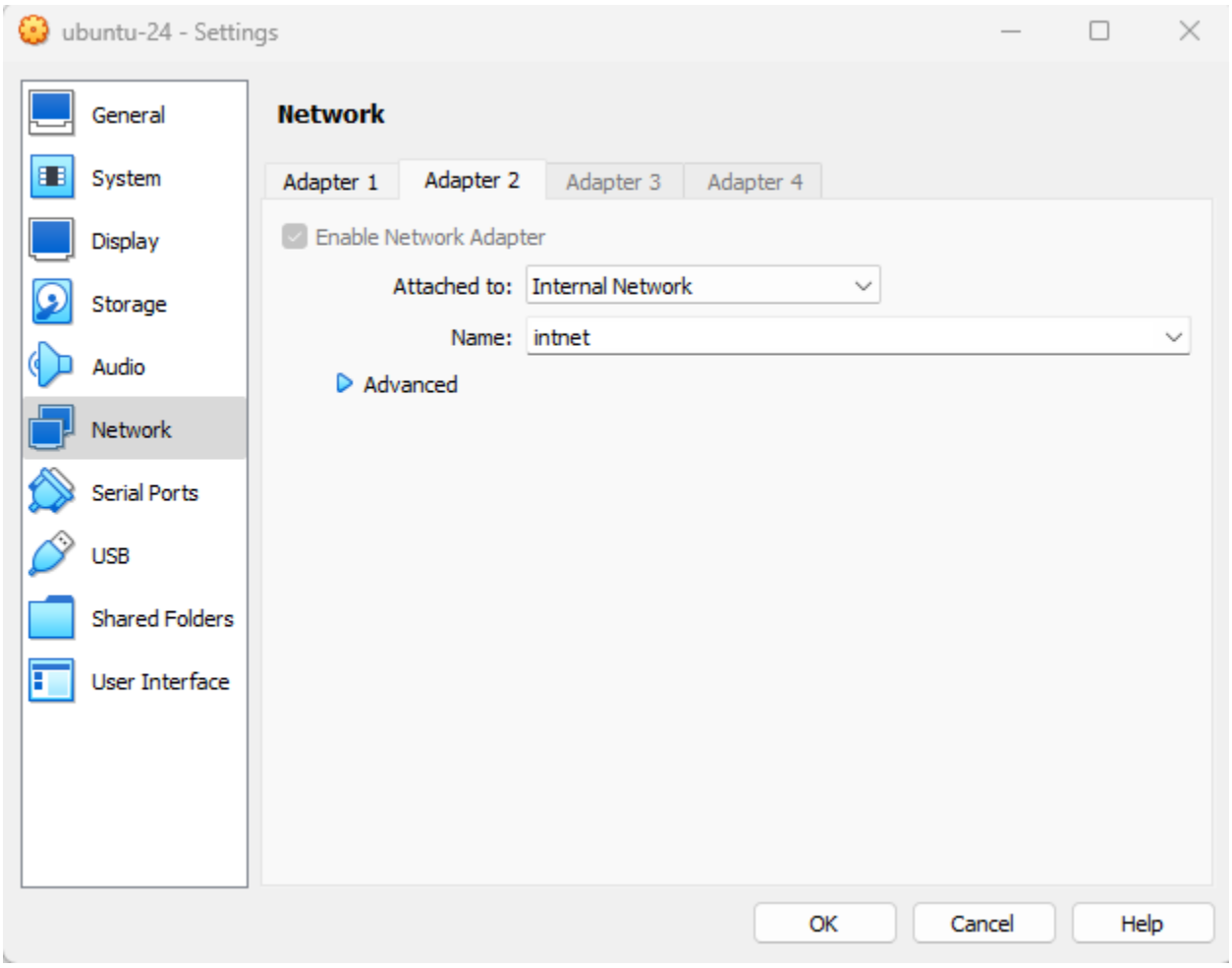
```
chanuli@chanuli-VirtualBox:~$ sudo apt update
[sudo] password for chanuli:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [374 kB]
Hit:5 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [528 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [81.3 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4,516 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [349 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [67.8 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [269 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [113 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [10.1 kB]
Get:14 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [127 kB]
Get:15 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8,352 B]
Get:16 http://lk.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [353 kB]
Get:17 http://lk.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [68.1 kB]
Get:18 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [368 kB]
Get:19 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [151 kB]
Get:20 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [14.3 kB]
Fetched 3,139 kB in 6s (495 kB/s)
Reading package lists... Done
```

```
chanuli@chanuli-VirtualBox:~$ sudo apt install isc-dhcp-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  avahi-autoipd isc-dhcp-client-ddns
The following NEW packages will be installed:
  isc-dhcp-client
0 upgraded, 1 newly installed, 0 to remove and 27 not upgraded.
Need to get 329 kB of archives.
After this operation, 881 kB of additional disk space will be used.
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-client amd64 4.4.3-P1-4ubuntu2 [329 kB]
Fetched 329 kB in 4s (84.8 kB/s)
Selecting previously unselected package isc-dhcp-client.
(Reading database ... 151181 files and directories currently installed.)
Preparing to unpack .../isc-dhcp-client_4.4.3-P1-4ubuntu2_amd64.deb ...
Unpacking isc-dhcp-client (4.4.3-P1-4ubuntu2) ...
Setting up isc-dhcp-client (4.4.3-P1-4ubuntu2) ...
Processing triggers for man-db (2.12.0-4build2) ...
```

```
chanuli@chanuli-VirtualBox:~$ dpkg -l | grep isc-dhcp-client
ii  isc-dhcp-client                          4.4.3-P1-4ubuntu2                  amd64        DHCP client for automati
cally obtaining an IP address
```

```
chanuli@chanuli-VirtualBox:~$ sudo netplan apply

** (generate:3599): WARNING **: 14:54:52.392: Permissions for /etc/netplan/01-netcfg.yaml are too open. Netplan configuration sh
ould NOT be accessible by others.

** (generate:3599): WARNING **: 14:54:52.392: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan con
figuration should NOT be accessible by others.

** (process:3598): WARNING **: 14:54:53.283: Permissions for /etc/netplan/01-netcfg.yaml are too open. Netplan configuration sho
uld NOT be accessible by others.

** (process:3598): WARNING **: 14:54:53.285: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan conf
iguration should NOT be accessible by others.

** (process:3598): WARNING **: 14:54:53.512: Permissions for /etc/netplan/01-netcfg.yaml are too open. Netplan configuration sho
uld NOT be accessible by others.

** (process:3598): WARNING **: 14:54:53.512: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan conf
iguration should NOT be accessible by others.
```






```
chanuli@chanuli-VirtualBox:~$ sudo dhclient enp0s8
```

```
chanuli@chanuli-VirtualBox:~$ ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
       valid_lft 453sec preferred_lft 453sec
    inet 192.168.56.104/24 brd 192.168.56.255 scope global secondary dynamic enp0s8
       valid_lft 492sec preferred_lft 492sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

```
chanuli@chanuli-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:90:55:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85892sec preferred_lft 85892sec
    inet6 fe80::a00:27ff:fe90:5555/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
       valid_lft 393sec preferred_lft 393sec
    inet 192.168.56.104/24 brd 192.168.56.255 scope global secondary dynamic enp0s8
       valid_lft 432sec preferred_lft 432sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

cat /var/lib/dhcp/dhclient.leases

```
chanuli@chanuli-VirtualBox:~$ cat /var/lib/dhcp/dhclient.leases
lease {
  interface "enp0s8";
  fixed-address 192.168.56.104;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 600;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.56.100;
  renew 4 2024/09/19 09:34:34;
  rebind 4 2024/09/19 09:39:18;
  expire 4 2024/09/19 09:40:33;
}
```

From server to client

```
chanuli@server:~$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.142 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.104 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.141 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.108 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.115 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.118 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.099 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=0.136 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.098 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=0.192 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=0.095 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=0.127 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=0.169 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=0.118 ms
64 bytes from 192.168.56.102: icmp_seq=15 ttl=64 time=0.101 ms
^C
--- 192.168.56.102 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14298ms
rtt min/avg/max/mdev = 0.095/0.124/0.192/0.026 ms
```

```
C:\Users\User>ping 192.168.56.102

Pinging 192.168.56.102 with 32 bytes of data:
Reply from 192.168.56.102: bytes=32 time<1ms TTL=64
Reply from 192.168.56.102: bytes=32 time=2ms TTL=64
Reply from 192.168.56.102: bytes=32 time=2ms TTL=64
Reply from 192.168.56.102: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.56.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Client to server

```
chanuli@server:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.048 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.130 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.148 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.323 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.110 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.120 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.120 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.134 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.120 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.135 ms
^C
--- 10.0.2.15 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10256ms
rtt min/avg/max/mdev = 0.048/0.132/0.323/0.066 ms
```

```
chanuli@server:/etc/dhcp$ dhcp-lease-list
To get manufacturer names please download http://standards-oui.ieee.org/oui.txt to /usr/lo
cal/etc/oui.txt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC               IP              hostname       valid until         manufacturer
==========================================================================================
=====
08:00:27:71:b8:87  10.0.2.100      server         2024-09-23 20:10:18 -NA-
```

```
chanuli@server:~$ cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.3-P1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 10.0.2.100 {
  starts 2 2024/09/24 18:08:57;
  ends 2 2024/09/24 18:18:57;
  tstp 2 2024/09/24 18:18:57;
  cltt 2 2024/09/24 18:08:57;
  binding state free;
  hardware ethernet 08:00:27:71:b8:87;
  uid "\001\010\000'q\270\207";
}
server-duid "\000\001\000\001.\204\351\211\010\000'\220UU";
```

The contents of the /var/lib/dhcp/dhcpd.leases file show that DHCP server has assigned a lease to a client.

Explanation of Lease Entry:

1. Lease Address: 10.0.2.100
   This is the IP address that was assigned by the DHCP server to the client.
2. Lease Time:
   - Starts: The time the lease started.
   - Ends: The time the lease expired.
   - TSTP: The time at which the lease was no longer valid (the end of the lease period).
   - CLTT: The time the DHCP server last communicated with the client.
3. UID: This is a unique identifier for the client.

What Does This Mean?

- The DHCP server is working because it has successfully assigned an IP address (10.0.2.100) to a client.

```
chanuli@server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:90:55:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85661sec preferred_lft 85661sec
    inet6 fe80::a00:27ff:fe90:5555/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
       valid_lft 585sec preferred_lft 585sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

```
chanuli@server:~$ sudo dhclient -r enp0s8
[sudo] password for chanuli:
chanuli@server:~$ ip a show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
chanuli@server:~$ sudo dhclient enp0s8
chanuli@server:~$ ip a show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic enp0s8
       valid_lft 594sec preferred_lft 594sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

```
chanuli@server:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.101 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.114 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.105 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.094 ms
^C
--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4102ms
rtt min/avg/max/mdev = 0.043/0.091/0.114/0.025 ms
```

```
chanuli@server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:90:55:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 84698sec preferred_lft 84698sec
    inet6 fe80::a00:27ff:fe90:5555/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.100/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s8
       valid_lft 509sec preferred_lft 509sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

```
chanuli@server:~$ dhcp-lease-list
To get manufacturer names please download http://standards-oui.ieee.org/oui.txt to /usr/local/etc/oui.t
xt
Reading leases from /var/lib/dhcp/dhcpd.leases
MAC                IP              hostname       valid until         manufacturer
=============================================================================================
08:00:27:71:b8:87  10.0.2.100      server         2024-09-25 08:09:34 -NA-
```

```
chanuli@server:~$ cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.3-P1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 10.0.2.100 {
  starts 2 2024/09/24 18:08:57;
  ends 2 2024/09/24 18:18:57;
  tstp 2 2024/09/24 18:18:57;
  cltt 2 2024/09/24 18:08:57;
  binding state free;
  hardware ethernet 08:00:27:71:b8:87;
  uid "\001\010\000'q\270\207";
}
server-duid "\000\001\000\001.\204\351\211\010\000'\220UU";

lease 10.0.2.100 {
  starts 3 2024/09/25 07:59:34;
  ends 3 2024/09/25 08:09:34;
  cltt 3 2024/09/25 07:59:34;
  binding state active;
  next binding state free;
```

```
lease 10.0.2.100 {
  starts 2 2024/09/24 18:08:57;
  ends 2 2024/09/24 18:18:57;
  tstp 2 2024/09/24 18:18:57;
  cltt 2 2024/09/24 18:08:57;
  binding state free;
  hardware ethernet 08:00:27:71:b8:87;
  uid "\001\010\000'q\270\207";
}
server-duid "\000\001\000\001.\204\351\211\010\000'\220UU";

lease 10.0.2.100 {
  starts 3 2024/09/25 07:59:34;
  ends 3 2024/09/25 08:09:34;
  cltt 3 2024/09/25 07:59:34;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:71:b8:87;
  uid "\001\010\000'q\270\207";
  client-hostname "server";
}
```

```
chanuli@server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:90:55:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 84162sec preferred_lft 84162sec
    inet6 fe80::a00:27ff:fe90:5555/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.101/24 brd 10.0.2.255 scope global dynamic enp0s8
       valid_lft 365sec preferred_lft 365sec
    inet 10.0.2.100/24 brd 10.0.2.255 scope global secondary dynamic noprefixroute enp0s8
       valid_lft 495sec preferred_lft 495sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

```
chanuli@server:~$ 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:fe90:5555  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:90:55:55  txqueuelen 1000  (Ethernet)
        RX packets 7805  bytes 10512468 (10.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4003  bytes 307443 (307.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.101  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe71:b887  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:71:b8:87  txqueuelen 1000  (Ethernet)
        RX packets 1320  bytes 138039 (138.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5029  bytes 482280 (482.2 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 1787  bytes 189874 (189.8 KB)
```

DNS (Domain Name System)

The Domain Name System (DNS) is like the internet's address book. It is the system that translates human-friendly domain names like "google.com" into the numerical IP addresses that computers use to locate and communicate with each other on the internet.

First, I change my server's name. Because, it is easier to manage and troubleshooting.

```
chanuli@chanuli-VirtualBox:~$ sudo hostnamectl set-hostname server.example.com
[sudo] password for chanuli:
```

```
~$ sudo nano /etc/hosts
```

```
  GNU nano 7.2                                          /etc/hosts *
127.0.0.1 localhost
127.0.1.1 server.example.com

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
$ sudo reboot
```

Step 1: Install bind9 DNS server

Update package list.

```
chanuli@server:~$ sudo apt update
[sudo] password for chanuli:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [377 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [81.4 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [353 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [68.1 kB]
Hit:8 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:9 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [530 kB]
Get:10 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [128 kB]
Get:11 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8,548 B]
Get:12 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [373 kB]
Get:13 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [153 kB]
Get:14 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [14.6 kB]
Fetched 2,339 kB in 4s (599 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
35 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

BIND (Berkeley Internet Name Domain) is one of the most widely used DNS server. This is how it install and configure it.

```
chanuli@server:~$ sudo apt install bind9 bind9utils bind9-doc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-utils
Suggested packages:
  bind-doc
The following NEW packages will be installed:
  bind9 bind9-doc bind9-utils bind9utils
0 upgraded, 4 newly installed, 0 to remove and 35 not upgraded.
Need to get 3,666 kB of archives.
After this operation, 8,936 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-utils amd64 1:9.18.28-0ubuntu0.24.04.1 [159 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9 amd64 1:9.18.28-0ubuntu0.24.04.1 [254 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 bind9-doc all 1:9.18.28-0ubuntu0.24.04.1 [3,249 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 bind9utils all 1:9.18.28-0ubuntu0.24.04.1 [3,682 B]
Fetched 3,666 kB in 3s (1,170 kB/s)
Selecting previously unselected package bind9-utils.
(Reading database ... 151206 files and directories currently installed.)
Preparing to unpack .../bind9-utils_1%3a9.18.28-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9-utils (1:9.18.28-0ubuntu0.24.04.1) ...
Selecting previously unselected package bind9.
Preparing to unpack .../bind9_1%3a9.18.28-0ubuntu0.24.04.1_amd64.deb ...
Unpacking bind9 (1:9.18.28-0ubuntu0.24.04.1) ...
```

Step 2: Configure BIND

```
chanuli@server:~$ sudo nano /etc/bind/named.conf.options
```

Add google public DNS server to the forward section. Uncomment the follow line to enable listening on all interfaces. “allow-query { any; };”

```
GNU nano 7.2                                  /etc/bind/named.conf.options *
      directory "/var/cache/bind";

      // If there is a firewall between you and nameservers you want
      // to talk to, you may need to fix the firewall to allow multiple
      // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

      // If your ISP provided one or more IP addresses for stable
      // nameservers, you probably want to use them as forwarders.
      // Uncomment the following block, and insert the addresses replacing
      // the all-0's placeholder.

       forwarders {
       8.8.8.8;    // Google's public DNS
       8.8.4.4;
             };
      allow-query { any; };    // Allows anyone to query the server


      //========================================================================
      // If BIND logs error messages about the root key being expired,
      // you will need to update your keys.  See https://www.isc.org/bind-keys
      //========================================================================
```

Step 3: Define a DNS zone

```
chanuli@server:~$ sudo nano /etc/bind/named.conf.local
```

```
  GNU nano 7.2                                        /etc/bind/named.conf.loc
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
};
```

The zone “example.com” tells the DNS server that it will handle requests for the domain example.com.

A master zone means that this DNS server holds the original(authoritative) copy of the zone data.

The server is responsible for maintaining and serving the DNS records for example.com directly.

- A record: Mapping domain names to IP addresses.

- NS records: Specifying the authoritative name servers.
- SOA (Start of Authority): Define authoritative information for the zone.

```
chanuli@server:~$ cd /etc/bind
chanuli@server:/etc/bind$ ls
bind.keys  db.127  db.empty  named.conf                named.conf.local    rndc.key
db.0       db.255  db.local  named.conf.default-zones  named.conf.options  zones.rfc1918
chanuli@server:/etc/bind$ cd
chanuli@server:~$ sudo cp /etc/bind/db.local /etc/bind/db.example.com
chanuli@server:~$ cd /etc/bind
chanuli@server:/etc/bind$ ls
bind.keys  db.127  db.empty        db.local    named.conf.default-zones  named.conf.options  zones.rfc1918
db.0       db.255  db.example.com  named.conf  named.conf.local          rndc.key
```

Create a zone file for example.com

```
chanuli@server:~$ sudo nano /etc/bind/db.example.com
```

```
                                                    chanuli@server: ~
  GNU nano 7.2                                  /etc/bind/db.example.com *
;
; BIND data file for server.example.com
;
$TTL    604800
@       IN      SOA     server.example.com. admin.example.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      server.example.com.
server  IN      A       10.0.2.15
@       IN      A       10.0.2.15
@       IN      AAAA    ::1
```

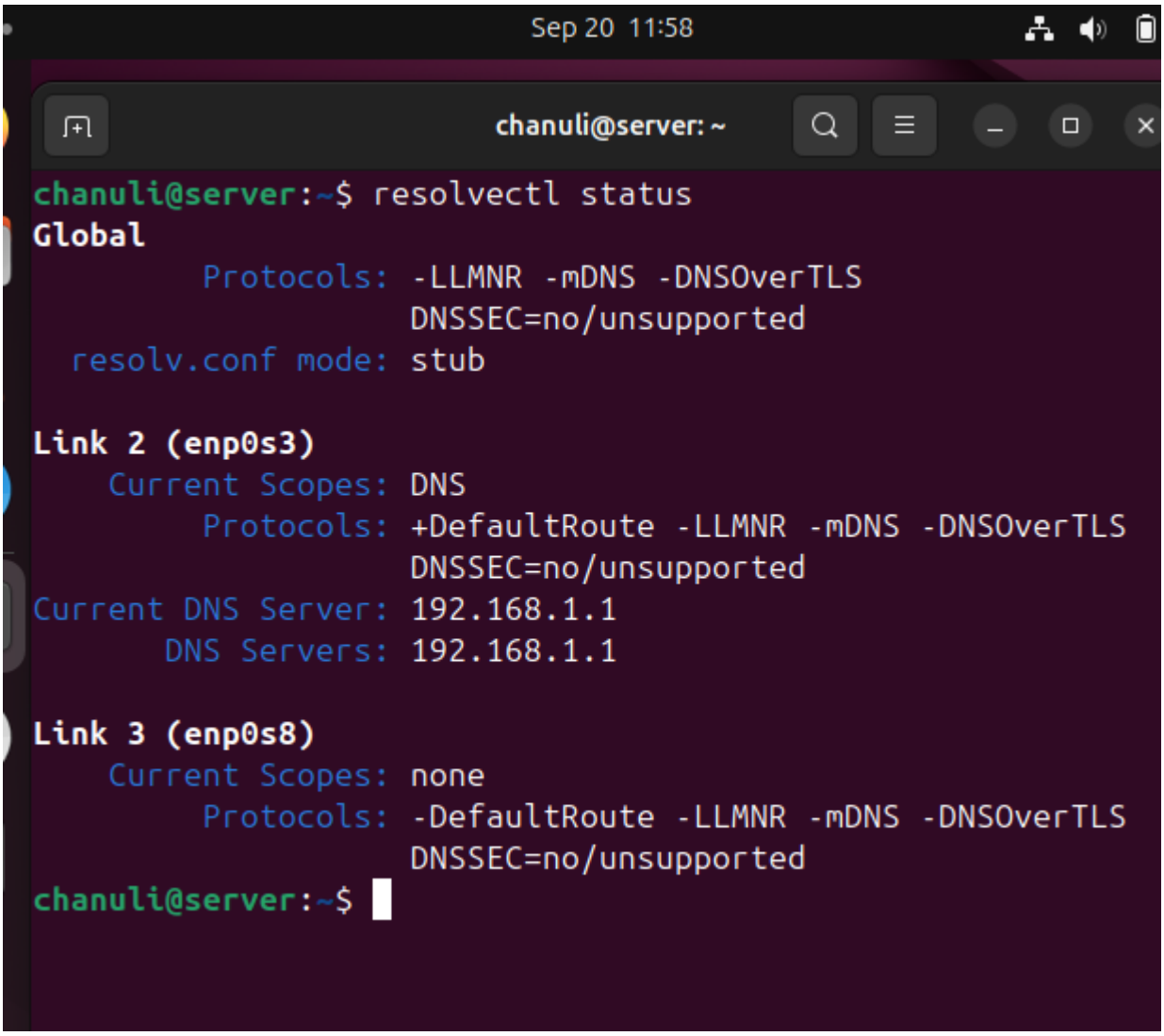
Step 4: Update Resolve.conf

Open the resolve.conf file to configure the local machine to use its DNS.

cat /etc/resolv.conf

```
chanuli@server:~$ cat /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search .
```

```
chanuli@server:~$ hostname -I
10.0.2.15 192.168.56.102
```



Step 2: Restart BIND and test

```
chanuli@server:~$ sudo systemctl restart bind9
```

```
chanuli@server:~$ sudo systemctl status bind9
[sudo] password for chanuli:
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-09-19 23:17:27 +0530; 55min ago
       Docs: man:named(8)
   Main PID: 4259 (named)
     Status: "running"
      Tasks: 8 (limit: 9446)
     Memory: 5.7M (peak: 6.1M)
        CPU: 78ms
     CGroup: /system.slice/named.service
             └─4259 /usr/sbin/named -f -u bind

Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Sep 19 23:17:27 server.example.com named[4259]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Sep 19 23:17:27 server.example.com named[4259]: running
Sep 19 23:17:28 server.example.com named[4259]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer comple>
Sep 19 23:17:28 server.example.com named[4259]: resolver priming query complete: success
chanuli@server:~$
```

Verification

nslookup is a program to query Internet domain name servers.

```
chanuli@server:~$ nslookup server.example.com localhost
Server:         localhost
Address:        127.0.0.1#53

Name:   server.example.com
Address: 10.0.2.15

chanuli@server:~$ nslookup server.example.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Name:   server.example.com
Address: 127.0.1.1
```

dig is a flexible tool for interrogating DNS name servers.

```
chanuli@server:~$ dig google.com

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22312
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             280     IN      A       172.253.118.101
google.com.             280     IN      A       172.253.118.138
google.com.             280     IN      A       172.253.118.139
google.com.             280     IN      A       172.253.118.102
google.com.             280     IN      A       172.253.118.113
google.com.             280     IN      A       172.253.118.100

;; Query time: 321 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Sep 26 20:18:13 +0530 2024
```

```
chanuli@server:~$ ping www.example.com
PING www.example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14: icmp_seq=1 ttl=53 time=408 ms
64 bytes from 93.184.215.14: icmp_seq=2 ttl=53 time=331 ms
64 bytes from 93.184.215.14: icmp_seq=3 ttl=53 time=252 ms
64 bytes from 93.184.215.14: icmp_seq=4 ttl=53 time=257 ms
^C
--- www.example.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3020ms
rtt min/avg/max/mdev = 251.979/311.992/408.227/63.830 ms
```

When we type this IP adders in any web browser like chrome, edge it loads to the google web site. It proves our DNS server provide the correct IP address.

```
chanuli@server:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.251.12.138
Name:   google.com
Address: 142.251.12.101
Name:   google.com
Address: 142.251.12.139
Name:   google.com
Address: 142.251.12.113
Name:   google.com
Address: 142.251.12.100
Name:   google.com
Address: 142.251.12.102
Name:   google.com
Address: 2404:6800:4003:c1c::65
Name:   google.com
Address: 2404:6800:4003:c1c::64
Name:   google.com
Address: 2404:6800:4003:c1c::8a
```

NTP (Network Time Protocols)

1.Install NTP package – This allows your machine to synchronize time with an external NTP server. The main purpose of NTP is to ensure that clock on computer and network devices remain accurate and synchronized across the network.

```
chanuli@server:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [530 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [373 kB]
Fetched 1,030 kB in 4s (232 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
23 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
chanuli@server:~$ sudo apt install ntp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ntpsec python3-ntp
Suggested packages:
  certbot ntpsec-doc ntpsec-ntpviz
The following packages will be REMOVED:
  systemd-timesyncd
The following NEW packages will be installed:
  ntp ntpsec python3-ntp
0 upgraded, 3 newly installed, 1 to remove and 23 not upgraded.
Need to get 450 kB of archives.
After this operation, 1,102 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 python3-ntp amd64 1.2.2+dfsg1-4build2
[91.2 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 ntpsec amd64 1.2.2+dfsg1-4build2 [343
kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/universe amd64 ntp all 1:4.2.8p15+dfsg-2~1.2.2+dfsg1-
4build2 [15.7 kB]
Fetched 450 kB in 4s (121 kB/s)
(Reading database ... 189367 files and directories currently installed.)
```

2.Configure NTP server

Edit NTP configuration file

```
chanuli@server:~$ cd /etc/systemd
chanuli@server:/etc/systemd$ ls
journald.conf  network        oomd.conf    resolved.conf  system       system-generators  user
logind.conf    networkd.conf  pstore.conf  sleep.conf     system.conf  timesyncd.conf     user.conf
chanuli@server:/etc/systemd$ nano timesyncd.conf
chanuli@server:/etc/systemd$ sudo nano timesyncd.conf
```

Verify NTP service – To ensure that the NTP service is running and synchronizing time correctly check its status.

```
chanuli@server:~$ sudo systemctl status ntp
● ntpsec.service - Network Time Service
     Loaded: loaded (/usr/lib/systemd/system/ntpsec.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-09-21 22:52:13 +0530; 2min 34s ago
       Docs: man:ntpd(8)
    Process: 16813 ExecStart=/usr/libexec/ntpsec/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
   Main PID: 16816 (ntpd)
      Tasks: 1 (limit: 9446)
     Memory: 10.5M (peak: 11.0M)
        CPU: 133ms
     CGroup: /system.slice/ntpsec.service
             └─16816 /usr/sbin/ntpd -p /run/ntpd.pid -c /etc/ntpsec/ntp.conf -g -N -u ntpsec:ntpsec

Sep 21 22:52:19 server.example.com ntpd[16816]: DNS: dns_check: processing ntp.ubuntu.com, 1, 20801
Sep 21 22:52:19 server.example.com ntpd[16816]: DNS: Server taking: 91.189.91.157
Sep 21 22:52:19 server.example.com ntpd[16816]: DNS: dns_take_status: ntp.ubuntu.com=>good, 0
Sep 21 22:52:20 server.example.com ntpd[16816]: DNS: dns_probe: 2.ubuntu.pool.ntp.org, cast_flags:8,>
Sep 21 22:52:21 server.example.com ntpd[16816]: DNS: dns_check: processing 2.ubuntu.pool.ntp.org, 8,>
Sep 21 22:52:21 server.example.com ntpd[16816]: DNS: Pool skipping: 162.159.200.123
Sep 21 22:52:21 server.example.com ntpd[16816]: DNS: Pool skipping: 162.159.200.1
Sep 21 22:52:21 server.example.com ntpd[16816]: DNS: Pool taking: 2606:4700:f1::1
Sep 21 22:52:21 server.example.com ntpd[16816]: DNS: Pool taking: 2606:4700:f1::123
Sep 21 22:52:21 server.example.com ntpd[16816]: DNS: dns_take_status: 2.ubuntu.pool.ntp.org=>good, 8
```

Check NTP synchronization

ntpq -p :query the Network Time Protocol (NTP) server status

```
chanuli@server:~$ sudo apt update
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [380
kB]
```

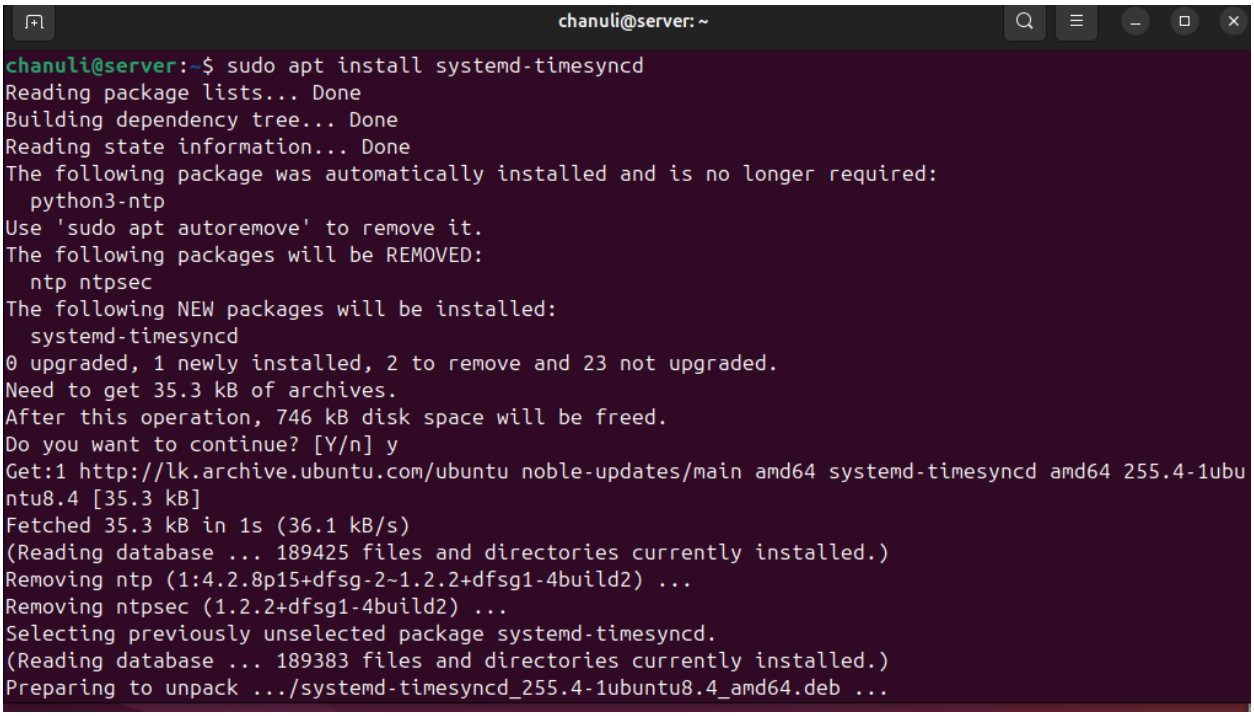
```
chanuli@server:~$ sudo apt install ntpsec
[sudo] password for chanuli:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  certbot ntpsec-doc ntpsec-ntpviz
The following packages will be REMOVED:
  systemd-timesyncd
The following NEW packages will be installed:
  ntpsec
```

```
chanuli@server:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
 0.ubuntu.pool.n .POOL.          16 p    -  256    0    0.0000    0.0000   0.0002
 1.ubuntu.pool.n .POOL.          16 p    -  256    0    0.0000    0.0000   0.0002
 2.ubuntu.pool.n .POOL.          16 p    -  256    0    0.0000    0.0000   0.0002
 3.ubuntu.pool.n .POOL.          16 p    -  256    0    0.0000    0.0000   0.0002
 prod-ntp-5.ntp1 201.68.88.106    2 u   15   64    1  242.3095   93.1774   0.0000
+time.cloudflare 10.237.8.6       3 u   10   64    1  190.0022   56.6940 107.4208
+time.cloudflare 10.237.8.6       3 u   10   64    1  190.0788   56.7032 110.2281
 time.cloudflare .INIT.          16 u    -   64    0    0.0000    0.0000   0.0002
 time.cloudflare .INIT.          16 u    -   64    0    0.0000    0.0000   0.0002
```

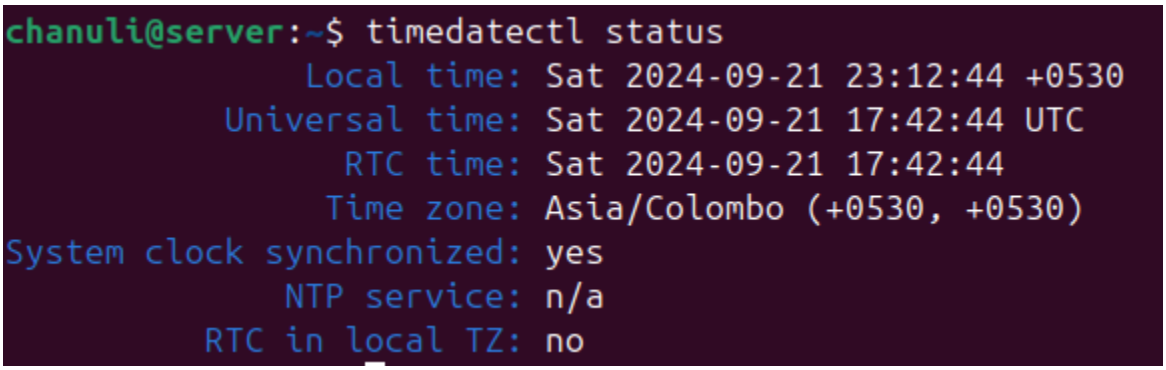
In my machine there was a message system-timesyncd.service not found. So, I have to install systemd-timesyncd package. This package is a lightweight NTP client that synchronizes the system clock with remote/public NTP servers.

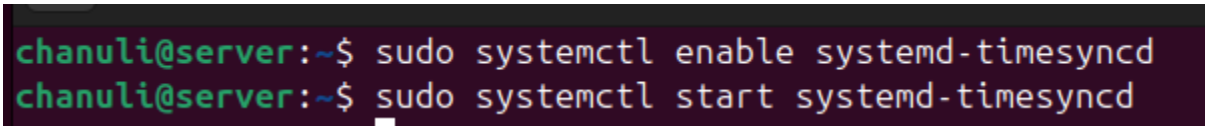
```
chanuli@server:/etc/systemd$ sudo systemctl restart systemd-timesyncd
Failed to restart systemd-timesyncd.service: Unit systemd-timesyncd.service not found.
chanuli@server:/etc/systemd$ sudo systemctl status systemd-timesyncd
Unit systemd-timesyncd.service could not be found.
```

```
chanuli@server:~$ sudo apt update
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 2s (52.8 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
23 packages can be upgraded. Run 'apt list --upgradable' to see them.
```



Check system time synchronization.





sudo systemctl status systemd-timesyncd

```
chanuli@server:~$ sudo systemctl status systemd-timesyncd
● systemd-timesyncd.service - Network Time Synchronization
     Loaded: loaded (/usr/lib/systemd/system/systemd-timesyncd.service; enabled>
     Active: active (running) since Fri 2024-09-27 12:47:31 +0530; 16s ago
       Docs: man:systemd-timesyncd.service(8)
   Main PID: 3853 (systemd-timesyn)
     Status: "Contacted time server 216.239.35.8:123 (time.google.com)."
      Tasks: 2 (limit: 9446)
     Memory: 1.4M (peak: 1.9M)
        CPU: 66ms
     CGroup: /system.slice/systemd-timesyncd.service
             └─3853 /usr/lib/systemd/systemd-timesyncd

Sep 27 12:47:31 server.example.com systemd[1]: Starting systemd-timesyncd.servi>
Sep 27 12:47:31 server.example.com systemd[1]: Started systemd-timesyncd.servic>
Sep 27 12:47:32 server.example.com systemd-timesyncd[3853]: Contacted time serv>
Sep 27 12:47:32 server.example.com systemd-timesyncd[3853]: Initial clock synch>
```

Verification

```
chanuli@server:~$ timedatectl status
               Local time: Sat 2024-09-21 23:33:19 +0530
           Universal time: Sat 2024-09-21 18:03:19 UTC
                 RTC time: Sat 2024-09-21 18:03:20
                Time zone: Asia/Colombo (+0530, +0530)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

3.Shell Scripting and Security

Shell Scripting

Script 1

```
chanuli@server:~$ pwd
/home/chanuli
```

```
chanuli@server:~$ mkdir system_reports
```

```
chanuli@server:~/system_reports$ nano report.sh
```

```
chanuli@server:~/system_reports$ ls
report.sh  system_reports_24-09-21.txt
```

```
chanuli@server:~/system_reports$ ls -al
total 16
drwxrwxr-x  2 chanuli chanuli 4096 Sep 21 02:52 .
drwxr-x--- 17 chanuli chanuli 4096 Sep 21 02:51 ..
-rw-rw-r--  1 chanuli chanuli  464 Sep 21 02:52 report.sh
-rw-rw-r--  1 chanuli chanuli  691 Sep 21 02:42 system_reports_24-09-21.txt
```

```
chanuli@server:~/system_reports$ chmod +x report.sh
chanuli@server:~/system_reports$ ls
report.sh  system_reports_24-09-21.txt
```

```
chanuli@server:~/system_reports$ ./report.sh
system report generated at /home/chanuli/system_reports/report_24-09-27.txt
```

Report.sh

```
#!/bin/bash

#create a variable to hold directory path

DIREC="/home/chanuli/system_reports"


#creat a directory if doesn't exit
```

```
mkdir -p "$DIREC"

#capture current date and store in a variable
CURRENT_DATE=$(date +"%y-%m-%d")

#full path to the report file including name and store in variable
REPORT_FILE="$DIREC/report_$CURRENT_DATE.txt"

#print system report
echo "system report for $(hostname)" > "$REPORT_FILE"

#print current date and time
echo "Date: $(date)" >> "$REPORT_FILE"

#print how long system is running
echo "uptime: $(uptime -p)" >> "$REPORT_FILE"

#print the free memory
echo "free mamory: " >> "$REPORT_FILE"

#display memory usage(total,used,free)
free -h >> "$REPORT_FILE"
```

#print disk usage details

echo "Disk usage: " >> "$REPORT_FILE"

#show disk space usage

df -h >> "$REPORT_FILE"

#print the successful message

echo "system report generated at $REPORT_FILE"

```
  GNU nano 7.2                                                report.sh *
#!/bin/bash

#create a variable to hold directory path
DIREC="/home/chanuli/system_reports"

#creat a directory if doesn't exit
mkdir -p "$DIREC"

#capture current date and store in a variable
CURRENT_DATE=$(date +"%y-%m-%d")

#full path to the report file including name and store in variable
REPORT_FILE="$DIREC/report_$CURRENT_DATE.txt"

#print system report
echo "system report for $(hostname)" > "$REPORT_FILE"

#print current date and time
echo "Date: $(date)" >> "$REPORT_FILE"

#print how long system is running
echo "uptime: $(uptime -p)" >> "$REPORT_FILE"
```

```
#print the free memory
echo "free mamory: " >> "$REPORT_FILE"

#display memory usage(total,used,free)
free -h >> "$REPORT_FILE"

#print disk usage details
echo "Disk usage: " >> "$REPORT_FILE"

#show disk space usage
df -h >> "$REPORT_FILE"

#print the successful message
echo "system report generated at $REPORT_FILE"
```

crontab -e

```
chanuli@server:~$ crontab -e
```

0 8 * * * /home/chanuli/system_reports/report.sh

This cron job will run the script /home/chanuli/system_reports/report.sh every day at 8:00 AM.

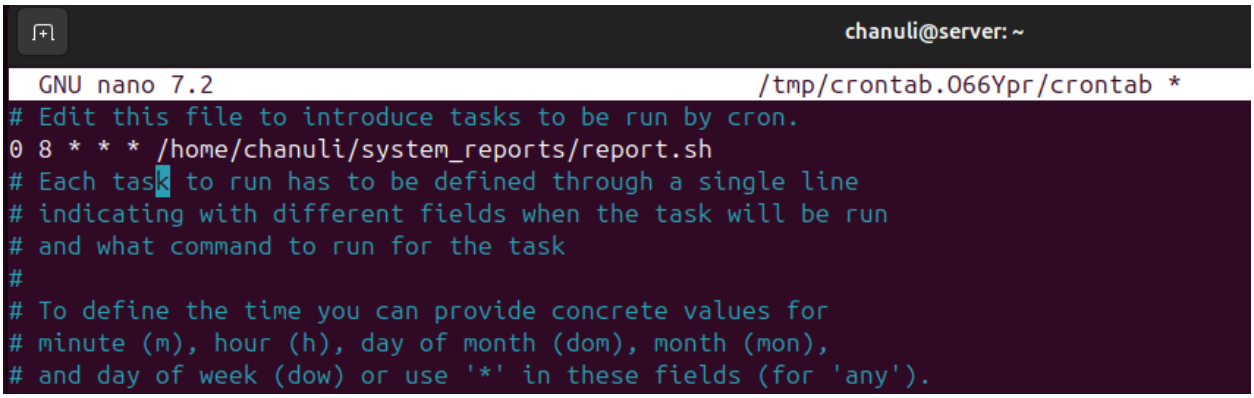
0: Minute (0th minute, so at the start of the hour)

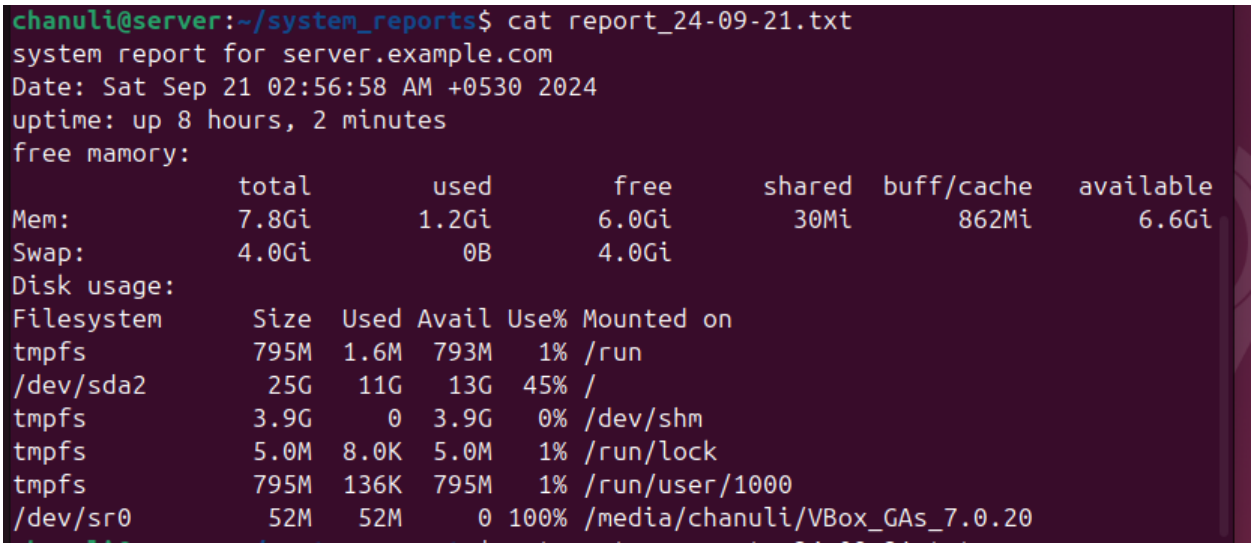
8: Hour (8 AM)

*: Day of the month (any day of the month)

*: Month (any month)

*: Day of the week (any day of the week)


chanuli@server: ~
GNU nano 7.2 /tmp/crontab.O66Ypr/crontab *
Edit this file to introduce tasks to be run by cron.
0 8 * * * /home/chanuli/system_reports/report.sh
Each task to run has to be defined through a single line
indicating with different fields when the task will be run
and what command to run for the task
#
To define the time you can provide concrete values for
minute (m), hour (h), day of month (dom), month (mon),
and day of week (dow) or use '*' in these fields (for 'any').


chanuli@server:~/system_reports$ cat report_24-09-21.txt
system report for server.example.com
Date: Sat Sep 21 02:56:58 AM +0530 2024
uptime: up 8 hours, 2 minutes
free mamory:
total used free shared buff/cache available
Mem: 7.8Gi 1.2Gi 6.0Gi 30Mi 862Mi 6.6Gi
Swap: 4.0Gi 0B 4.0Gi
Disk usage:
Filesystem Size Used Avail Use% Mounted on
tmpfs 795M 1.6M 793M 1% /run
/dev/sda2 25G 11G 13G 45% /
tmpfs 3.9G 0 3.9G 0% /dev/shm
tmpfs 5.0M 8.0K 5.0M 1% /run/lock
tmpfs 795M 136K 795M 1% /run/user/1000
/dev/sr0 52M 52M 0 100% /media/chanuli/VBox_GAs_7.0.20

Script 2

```
chanuli@server:~$ cd Documents
chanuli@server:~/Documents$ ls
file.sh
chanuli@server:~/Documents$ ./file.sh
bash: ./file.sh: Permission denied
chanuli@server:~/Documents$ chmod +x file.sh
chanuli@server:~/Documents$ ls
file.sh
```

```
chanuli@server:~/Documents$ nano file.sh
```

chanuli@server: ~/Documents

```
  GNU nano 7.2                                  file.sh
#!/bin/bash

#hold the path to the source directory
SOURCE="/home/chanuli/Documents"

#hold the path to the destination directory
DES="/home/chanuli/backup/Documents"

#check directory is exit if not create
mkdir -p "$DES"

#store current date
CURRENT_DATE=$(date +"%y-%m-%d")

#store full path and name of the backup file
BACKUP="$DES/doc_backup_$CURRENT_DATE.txt"

#list all files and directory from source
ls -R "$SOURCE" > "$BACKUP"
```

```
#copy source to destination
cp -r "$SOURCE"/* "$DES/"

#sucussful message
echo "Backup created at $BACKUP"
```

file.sh

#!/bin/bash

#hold the path to the source directory

SOURCE="/home/chanuli/Documents"

#hold the path to the destination directory

DES="/home/chanuli/backup/Documents"

#check directory is exit if not create

mkdir -p "$DES"

#store current date

CURRENT_DATE=$(date +"%y-%m-%d")

#store full path and name of the backup file

BACKUP="$DES/doc_backup_$CURRENT_DATE.txt"

#list all files and directory from source

ls -R "$SOURCE" > "$BACKUP"

#copy source to destination

cp -r "$SOURCE"/* "$DES/"

#sucussful message

echo "Backup created at $BACKUP"

```
chanuli@server:~/Documents$ ./file.sh
Backup created at /home/chanuli/backup/Documents/doc_backup_24-09-21.txt
```

```
chanuli@server:~$ ls
backup    Documents  Music     Public  snp             Templates
Desktop   Downloads  Pictures  snap    system_reports  Videos
```

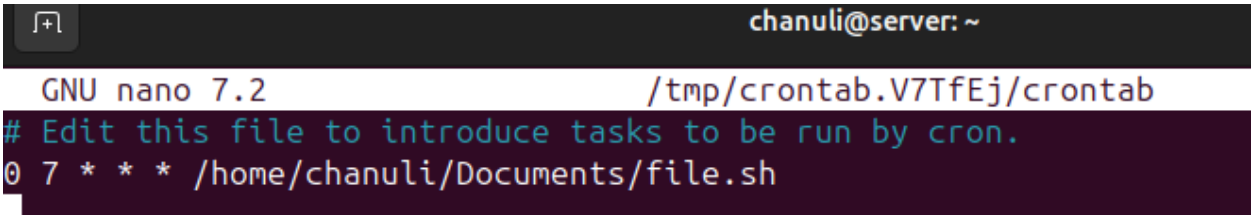
```
chanuli@server:~/Documents$ cd
chanuli@server:~$ cd backup
chanuli@server:~/backup$ cd Documents
chanuli@server:~/backup/Documents$ ls
back.txt  doc_backup_24-09-21.tar.gz  doc_backup_24-09-21.txt  file.sh  SNP
chanuli@server:~/backup/Documents$ cat doc_backup_24-09-21.txt
/home/chanuli/Documents:
file.sh
SNP

/home/chanuli/Documents/SNP:
rep.sh
```

crontab -e

```
chanuli@server:~$ crontab -e
crontab: installing new crontab
```

0 7 * * * /home/chanuli/Documents/file.sh

This cron job is scheduled to run the script /home/chanuli/Documents/file.sh every day at 7:00 AM.



SSH (Secure Shell)

SSH (Secure Shell) is a cryptographic network protocol used to securely access and manage remote systems over an unsecured network. SSH provides a secure communication channel between the client and server by encrypting the data transfer preventing eavesdropping, man-in-the-middle attack.

Step 1: Install OpenSSH server

```
chanuli@server:~$ sudo apt update
[sudo] password for chanuli:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 5s (27.4 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
23 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
chanuli@server:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-ntp
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 23 not upgraded.
Need to get 832 kB of archives.
After this operation, 6,747 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-sftp-server amd64 1:9.6p1-
3ubuntu13.5 [37.3 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 openssh-server amd64 1:9.6p1-3ubun
tu13.5 [509 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 ncurses-term all 6.4+20240113-1ubuntu2 [27
5 kB]
Get:4 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 ssh-import-id all 5.11-0ubuntu2 [10.0 kB]
```

Verify that the SSH server running. If it is inactive start and enable it.

```
chanuli@server:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
```

```
chanuli@server:~$ sudo systemctl start ssh
chanuli@server:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-instal
l.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/systemd/system/ssh
.service.
```

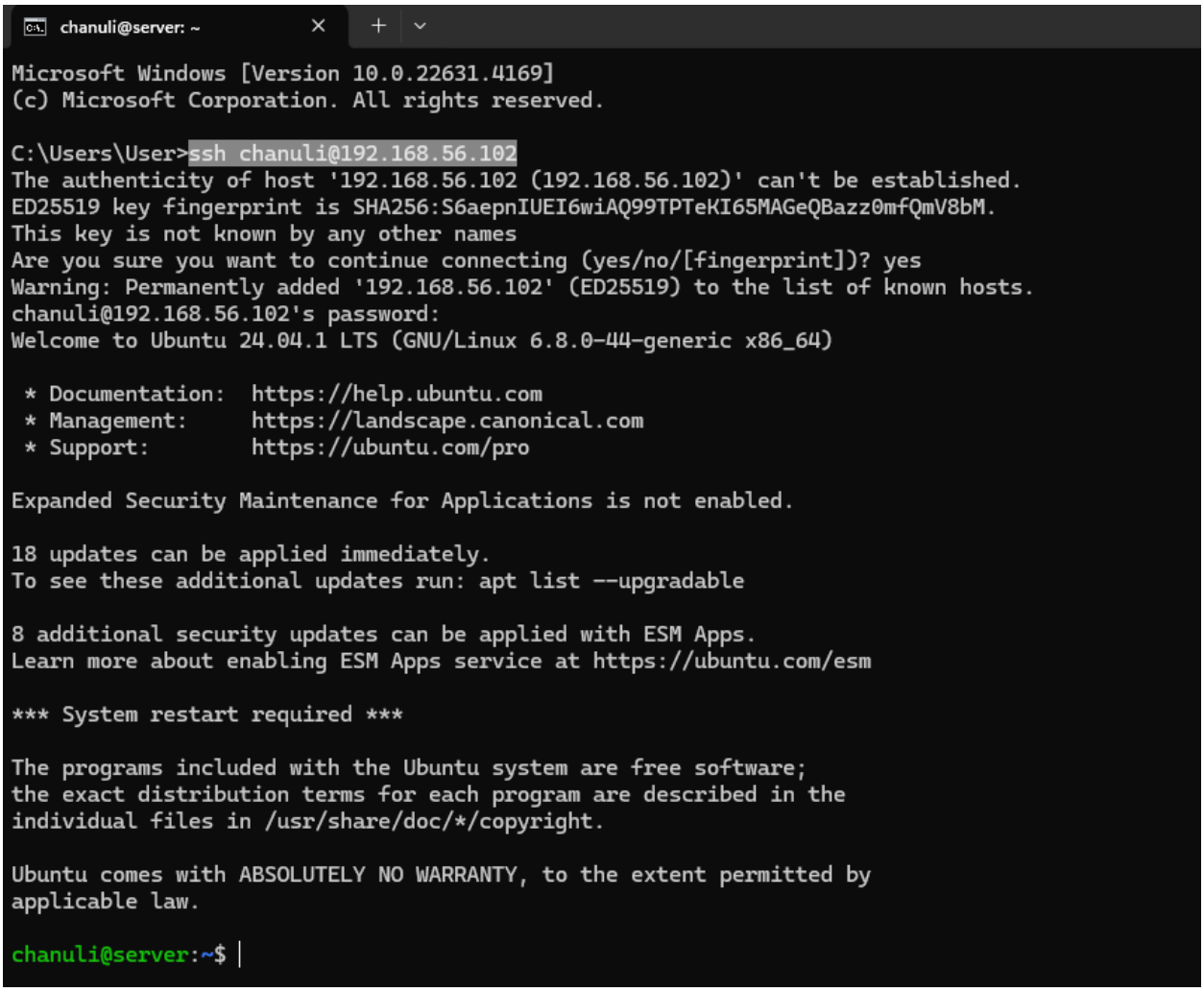
```
chanuli@server:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-09-22 00:57:15 +0530; 41s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 19723 (sshd)
      Tasks: 1 (limit: 9446)
     Memory: 1.2M (peak: 1.5M)
        CPU: 28ms
     CGroup: /system.slice/ssh.service
             └─19723 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 22 00:57:15 server.example.com systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 22 00:57:15 server.example.com sshd[19723]: Server listening on :: port 22.
Sep 22 00:57:15 server.example.com systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

```
chanuli@server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 08:00:27:90:55:55 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85147sec preferred_lft 85147sec
    inet6 fe80::a00:27ff:fe90:5555/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 08:00:27:71:b8:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
       valid_lft 328sec preferred_lft 328sec
    inet6 fe80::a00:27ff:fe71:b887/64 scope link
       valid_lft forever preferred_lft forever
```

Verification

Now, we can connect our ubuntu virtual machine remotely using another computer. This is how I access my ubuntu virtual machine using windows terminal.

Syntax: ssh username@server_IP



```
chanuli@server:~$ 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:fe90:5555  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:90:55:55  txqueuelen 1000  (Ethernet)
        RX packets 181084  bytes 254528695 (254.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 53898  bytes 3339286 (3.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe71:b887  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:71:b8:87  txqueuelen 1000  (Ethernet)
        RX packets 3382  bytes 483601 (483.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 354  bytes 57759 (57.7 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 1238  bytes 116857 (116.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1238  bytes 116857 (116.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

chanuli@server:~$ ls
backup  Desktop  Documents  Downloads  Music  Pictures  Public  snap  snp  system_reports  Templates  Videos
chanuli@server:~$
```

Iptables and ACLs

It is already pre-installed.

```
chanuli@server:~$ iptables --version
iptables v1.8.10 (nf_tables)
```

These are the current rules.

```
chanuli@server:~$ sudo iptables -L -v
[sudo] password for chanuli:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Flush all rules

sudo iptables -F – when run this command it removes all rules from all chains (INPUT, OUTPUT and FORWARD) without changing the default policies of these chains.

Flushing the rules will make the server unprotected until new rules are applied, especially if the default policies are set to ACCEPT. If the default policy is DROP flushing all rules will block all incoming connections unless new rules are defined.

sudo iptables -F

```
chanuli@server:~$ sudo iptables -F
[sudo] password for chanuli:
chanuli@server:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Set default policy

sudo iptables -P INPUT DROP – This command sets the default policy for the INPUT chain to DROP, which means that any incoming packet that doesn't match an explicit rule in the INPUT chain will be dropped.

sudo iptables -P FORWARD DROP – The FORWARD chain deals with packets that are routed through your system (our server is acting as a router). With this policy, unless you explicitly allow certain forwarding rules, all routed packets will be dropped.

sudo iptables -P OUTPUT ACCEPT – This sets the default policy for the OUTPUT chain to ACCEPT, it means that all outgoing traffic from your server will be allowed by default unless otherwise specified.

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

```
chanuli@server:~$ sudo iptables -P INPUT DROP
chanuli@server:~$ sudo iptables -P FORWARD DROP
chanuli@server:~$ sudo iptables -P OUTPUT ACCEPT
```

```
chanuli@server:~$ sudo iptables -L -v
Chain INPUT (policy DROP 85 packets, 18582 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 80 packets, 6769 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Web server security

Allow HTTP (Port 80) and HTTPS (port 443)

sudo iptables -P INPUT DROP

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

sudo netfilter-persistent save

sudo netfilter-persistent reload

```
chanuli@server:~$ sudo iptables -P INPUT DROP
chanuli@server:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
chanuli@server:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

```
chanuli@server:~$ sudo netfilter-persistent reload
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables star
t
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables star
t
```

sudo cat /etc/iptables/rules.v4

```
chanuli@server:~$ cat /etc/iptables/rules.v4
```

```
-A INPUT -j ufw-track-input
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

```
chanuli@server:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Allow DNS server

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

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

sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT

```
chanuli@server:~$ sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT
[sudo] password for chanuli:
chanuli@server:~$ sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT
chanuli@server:~$ sudo iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
chanuli@server:~$ sudo iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
```

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

```
chanuli@server:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
 ACCEPT
```

sudo netfilter-persistent save

```
chanuli@server:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

```
2   150 ACCEPT     udp  --  any    any     anywhere             anywhere
     udp dpt:domain
0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere
     tcp dpt:domain
```

```
chanuli@server:~$ sudo cat /etc/iptables/rules.v4
```

```
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Install apache web server

```
chanuli@server:~$ sudo apt update
[sudo] password for chanuli:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 12s (10.6 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
52 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

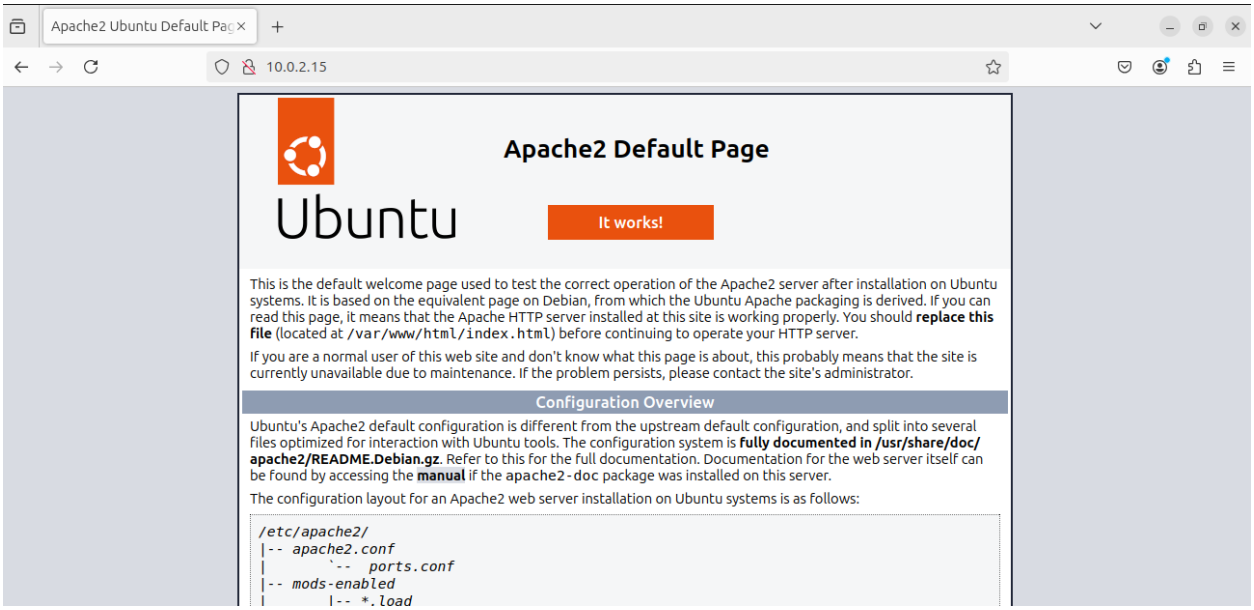
```
chanuli@server:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-ntp
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
0 upgraded, 8 newly installed, 0 to remove and 52 not upgraded.
Need to get 1,900 kB of archives.
After this operation, 7,455 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2
-3.1ubuntu0.1 [108 kB]
Get:2 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1
ubuntu7 [91.9 kB]
Get:3 http://lk.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64
```

sudo systemctl status apache2

```
chanuli@server:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-09-28 16:42:30 +0530; 5min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 15553 (apache2)
      Tasks: 55 (limit: 9446)
     Memory: 5.4M (peak: 5.8M)
        CPU: 61ms
     CGroup: /system.slice/apache2.service
             ├─15553 /usr/sbin/apache2 -k start
             ├─15555 /usr/sbin/apache2 -k start
             └─15556 /usr/sbin/apache2 -k start

Sep 28 16:42:30 server.example.com systemd[1]: Starting apache2.service - The Apache HTT>
Sep 28 16:42:30 server.example.com systemd[1]: Started apache2.service - The Apache HTTP>
```

Open your web browser and type this in search bar. http://your_server_ip

http://10.0.2.15



Check apache is listening to port 80

sudo netstat -tuln | grep :80

```
chanuli@server:~$ sudo netstat -tuln | grep :80
tcp6       0      0 ::::80                  :::*                    LISTEN
```

```
chanuli@server:~$ curl http://10.0.2.15
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Ubuntu, Verdana, sans-serif;
```

```
        <div class="section_header">
          <div id="bugs"></div>
                Reporting Problems
        </div>
        <div class="content_section_text">
          <p>
                Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
                Apache2 package with Ubuntu. However, check <a
                href="https://bugs.launchpad.net/ubuntu/+source/apache2"
                rel="nofollow">existing bug reports</a> before reporting a new bug.
          </p>
          <p>
                Please report bugs specific to modules (such as PHP and others)
                to their respective packages, not to the web server itself.
          </p>
        </div>

      </div>
    </div>
    <div class="validator">
    </div>
  </body>
</html>
```

curl -I http://10.0.2.15

```
chanuli@server:~$ curl -I http://10.0.2.15
HTTP/1.1 200 OK
Date: Sat, 28 Sep 2024 11:46:59 GMT
Server: Apache/2.4.58 (Ubuntu)
Last-Modified: Sat, 28 Sep 2024 11:12:27 GMT
ETag: "29af-6232c0c07b801"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html
```

```
chanuli@server:~$ curl -I http://192.168.56.102
HTTP/1.1 200 OK
Date: Sat, 28 Sep 2024 11:48:52 GMT
Server: Apache/2.4.58 (Ubuntu)
Last-Modified: Sat, 28 Sep 2024 11:12:27 GMT
ETag: "29af-6232c0c07b801"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html
```

https

sudo a2enmod ssl

a2enmod: A script provided by Apache to enable modules.

ssl: Refers to the SSL (Secure Sockets Layer) module, which enables Apache to support HTTPS (secure HTTP).

```
chanuli@server:~$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

sudo systemctl restart apache2

```
chanuli@server:~$ sudo systemctl restart apache2
```

sudo netstat -tuln | grep 443

```
chanuli@server:~$ sudo netstat -tuln | grep 443
tcp6       0      0 :::443                  :::*                    LISTEN
```

curl -I https://www.google.com

```
chanuli@server:~$ curl -I https://www.google.com
HTTP/2 200
content-type: text/html; charset=ISO-8859-1
content-security-policy-report-only: object-src 'none';base-uri 'self';script-sr
c 'nonce-Hl59gR8_V_-admB4Y2WXag' 'strict-dynamic' 'report-sample' 'unsafe-eval'
'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
-hp
accept-ch: Sec-CH-Prefers-Color-Scheme
p3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
date: Sat, 28 Sep 2024 20:33:15 GMT
server: gws
x-xss-protection: 0
x-frame-options: SAMEORIGIN
expires: Sat, 28 Sep 2024 20:33:15 GMT
cache-control: private
set-cookie: AEC=AVYB7cpHGGcY3oc2mLB31EVq43aO6kdoG152pVlICS4y9Gdtvbgpt3C3oGk; exp
ires=Thu, 27-Mar-2025 20:33:15 GMT; path=/; domain=.google.com; Secure; HttpOnly
; SameSite=lax
set-cookie: NID=518=WnKSrgNW2bweWs0EiQfsUf2N_wrcv0qpK4JgM3vPnSQToI2_7qH-nLUI3vFq
fCiMsSwGNp9SPo-Hr09nDqs8iJD2ecApz8y8rkIX7sYjtagac8d-HchYC7HTSJx3toMu-F_5upxDHEGl
b9KfVRK7m32XUzUzkehIK7QwhuqoFyBv1cvaOHVQwQoy75TuFC4; expires=Sun, 30-Mar-2025 20
:33:15 GMT; path=/; domain=.google.com; HttpOnly
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

- HTTP/2 200:This indicates that the server responded successfully (HTTP status code 200) and is using the HTTP/2 protocol.

```
chanuli@server:~$ curl -I https://google.com
HTTP/2 301
location: https://www.google.com/
content-type: text/html; charset=UTF-8
content-security-policy-report-only: object-src 'none';base-uri 'self';script-sr
c 'nonce-L40dNXAzkM9cXjBWTWJ0Lg' 'strict-dynamic' 'report-sample' 'unsafe-eval'
'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
-hp
date: Sun, 29 Sep 2024 02:09:04 GMT
expires: Tue, 29 Oct 2024 02:09:04 GMT
cache-control: public, max-age=2592000
server: gws
content-length: 220
x-xss-protection: 0
x-frame-options: SAMEORIGIN
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

Remote administration access

Allow SSH (port 22)

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

- -A : Appends(adds) a new rule to the end of the specified chain.
- -p tcp : Specifies the protocol being matched, TCP(Transmission Control Protocol) which is commonly used for network services like SSH, HTTP.
- –dport (destination port): Specifies the port number the packet is trying to reach.
- 22: SSH use default port 22
- -j: Stands for jump and specifies the target action.
- ACCEPT: The action to accept and allow the packet if it matches the rule.

sudo iptables -P INPUT ACCEPT

sudo iptables -A INPUT -p tcp -s 192.168.56.103 --dport 22 -j ACCEPT

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

```
chanuli@server:~$ sudo iptables -P INPUT ACCEPT
[sudo] password for chanuli:
chanuli@server:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.103 --dport 22 -j
ACCEPT
chanuli@server:~$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

sudo iptables-save | sudo tee /etc/iptables/rules.v4

```
chanuli@server:~$ sudo iptables-save | sudo tee /etc/iptables/rules.v4
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Sep 29 00:47:02 2024
*filter
:INPUT ACCEPT [248:34788]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [3124:317271]
-A INPUT -s 192.168.56.103/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
COMMIT
# Completed on Sun Sep 29 00:47:02 2024
```

```
chanuli@server:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.56.103       anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

sudo systemctl restart ssh

```
chanuli@server:~$ sudo systemctl restart ssh
```

```
C:\Users\User>ssh chanuli@192.168.56.102
chanuli@192.168.56.102's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

47 updates can be applied immediately.
18 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

8 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Sat Sep 28 23:48:28 2024 from 192.168.56.103
```

sudo netstat -tuln | grep 22

```
chanuli@server:~$ sudo netstat -tuln | grep 22
tcp6       0      0 :::22                   :::*                    LISTEN
```

Allow specific applications

Allow traffic on port 443

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

Allow outgoing traffic on port 443

sudo iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT

```
chanuli@server:~$ sudo iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT
```

Save the rules

sudo netfilter-persistent save

```
chanuli@server:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

sudo netstat -tuln | grep :443

```
chanuli@server:~$ sudo netstat -tuln | grep :443
[sudo] password for chanuli:
tcp6       0      0 ::443                   :::*                    LISTEN
```

```
chanuli@server:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.56.103       anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTA
BLISHED

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:https
```

Allow DHCP

Allow incoming DHCP requests (UDP port 67) to the DHCP server

sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT

Allow outgoing DHCP requests (UDP port 68) from the client

sudo iptables -A OUTPUT -p udp --dport 68 -j ACCEPT

```
chanuli@server:~$ sudo iptables -A INPUT -p udp --dport 67 -j ACCEPT
chanuli@server:~$ sudo iptables -A OUTPUT -p udp --dport 68 -j ACCEPT
```

Allow incoming DHCP responses to the client (UDP port 68)

sudo iptables -A INPUT -p udp --sport 67 --dport 68 -j ACCEPT

```
chanuli@server:~$ sudo iptables -A INPUT -p udp --sport 67 --dport 68 -j ACCEPT
```

sudo netfilter-persistent save

```
chanuli@server:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

```
chanuli@server:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 741 packets, 69147 bytes)
 pkts bytes target     prot opt in     out     source               destination
   60  9075 ACCEPT     6    --  *      *       192.168.56.103       0.0.0.0/0           tcp dpt:22
    0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   29  2208 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   81  9698 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
 3165 1080K ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
 1127 93632 ACCEPT     17   --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
    0     0 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    3   252 ACCEPT     1    --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8
    0     0 ACCEPT     17   --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:67
    0     0 ACCEPT     17   --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:67 dpt:68

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 3081 packets, 384K bytes)
 pkts bytes target     prot opt in     out     source               destination
 2065  163K ACCEPT     17   --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
  560 33920 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   41 20696 ACCEPT     6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
    0     0 ACCEPT     17   --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:68
```

Allow pings

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

```
chanuli@server:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACC
EPT
[sudo] password for chanuli:
```

sudo iptables-save | sudo tee /etc/iptables/rules.v4

```
chanuli@server:~$ sudo iptables-save | sudo tee /etc/iptables/rules.v4
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Sep 29 08:24:47 2024
*filter
:INPUT DROP [562:51375]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2707:346321]
-A INPUT -s 192.168.56.103/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 443 -j ACCEPT
COMMIT
# Completed on Sun Sep 29 08:24:47 2024
```

```
chanuli@server:~$ ping google.com
PING google.com (142.251.10.101) 56(84) bytes of data.
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=1 ttl=102 time=92.
3 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=2 ttl=102 time=56.
4 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=3 ttl=102 time=58.
0 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=4 ttl=102 time=54.
6 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=5 ttl=102 time=54.
0 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=6 ttl=102 time=73.
6 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=7 ttl=102 time=54.
8 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=8 ttl=102 time=74.
7 ms
64 bytes from sd-in-f101.1e100.net (142.251.10.101): icmp_seq=9 ttl=102 time=73.
5 ms
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8101ms
rtt min/avg/max/mdev = 53.990/65.761/92.342/12.630 ms
```

Printer server access

Allow Printing Traffic from Specific IP Addresses in Local Network

sudo iptables -A INPUT -p tcp -s 192.168.56.102 --dport 9100 -j ACCEPT

block external access to printer server on port 9100

sudo iptables -A INPUT -p tcp --dport 9100 -j DROP

```
chanuli@server:~$ sudo iptables -A INPUT -p tcp -s 192.168.56.102 --dport 9100 -j ACCEPT
chanuli@server:~$ sudo iptables -A INPUT -p tcp --dport 9100 -j DROP
```

Save Your iptables Rules

sudo sh -c "iptables-save > /etc/iptables/rules.v4"

```
chanuli@server:~$ sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

sudo netfilter-persistent save

```
chanuli@server:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

netstat -tuln | grep "9100"

```
chanuli@server:~$ netstat -tuln | grep "9100"
tcp        0      0 0.0.0.0:9100            0.0.0.0:*               LISTEN
```

```
chanuli@server:~$ sudo iptables -L -v
Chain INPUT (policy DROP 116 packets, 16025 bytes)
 pkts bytes target     prot opt in     out     source               destination
   25  3297 ACCEPT     tcp  --  any    any     192.168.56.103       anywhere             tcp dpt:ssh
    0     0 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
   29  2266 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
  221 30430 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  any    any     anywhere             anywhere             icmp echo-request
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootps
    6  3456 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:bootps dpt:bootpc
    2   120 ACCEPT     tcp  --  any    any     server.example.com   anywhere             tcp dpt:9100
   19  1140 DROP       tcp  --  any    any     anywhere             anywhere             tcp dpt:9100

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 232 packets, 29160 bytes)
 pkts bytes target     prot opt in     out     source               destination
   69  5171 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:https
```

sudo nc -l -p 9100

```
chanuli@server:~$ sudo nc -l -p 9100
[sudo] password for chanuli:
print server test sucessfull
```

echo "print server test sucessfull" | nc 192.168.56.102 9100

```
chanuli@server:~$ echo "print server test sucessfull" | nc 192.168.56.102 9100
```

4.Best Practices

1) Regularly update your system

By regularly updating the system, can ensure it stays protected against known threats and continues to operate securely.

sudo apt update

```
chanuli@server:~$ sudo apt update
[sudo] password for chanuli:
Hit:1 http://lk.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://lk.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [535 kB]
Get:6 http://lk.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [130 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [380 kB]
Get:8 http://lk.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8,672 B]
Get:9 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [379 kB]
Get:10 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [156 kB]
Get:11 http://lk.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [14.8 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [83.1 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4,576 B]
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [274 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [116 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [10.4 kB]
Fetched 2,344 kB in 7s (340 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
35 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

These are the some benefits we can gain by updating the system.

- Vulnerability Patches: Software developers regularly identify security vulnerabilities in operating systems, applications, and firmware. These vulnerabilities can be exploited by hackers to gain unauthorized access, spread malware, or execute other malicious activities. Updates contain patches that fix these weaknesses.
- Improved Security Features: Updates often include new security features or improvements to existing ones. These features help to protect your system from evolving threats like more sophisticated viruses, phishing attempts, and malware.
- Protection Against Zero-Day Exploits: Zero-day vulnerabilities are security flaws that are exploited by attackers before the vendor knows about them. Once discovered, vendors

release patches to mitigate the risks. If a system isn't updated, it remains exposed to these exploits.

- Bug Fixes: Updates frequently address bugs or errors in the software that could unintentionally weaken security, leading to potential data leaks or enabling attackers to bypass defenses.
- Malware Defense: Outdated systems are more vulnerable to malware infections since many security updates include improvements to antivirus or anti-malware capabilities.
- Compliance and Legal Obligations: Some industries have regulations that require systems to be kept up-to-date to meet security standards. Failure to do so can result in penalties or legal liability if a breach occurs.

2) Limit network access with firewalls

Configuring a firewall using iptables or ufw ensures only trusted connections can access network services. A common approach is to allow only necessary ports, such as SSH (port 22), HTTP (port 80), HTTPS (port 443) and other trusted ports.

These are some benefits using firewalls:

- Reduces Attack Surface: Firewalls block unauthorized access by only allowing necessary traffic based on predefined rules. This reduces the number of entry points that attackers can exploit.
- Prevents Unauthorized Access: Firewalls enforce strict access control, ensuring that only trusted devices and users can connect to critical services and resources, thus minimizing the risk of intrusion.
- Protects Web Servers and Remote Access: For services like web servers (HTTP, HTTPS), firewalls can restrict access to specific IP addresses or geographical regions, securing sensitive data and preventing unauthorized remote access.
- Filters Malicious Traffic: Firewalls can filter out malicious traffic (e.g., malware, phishing attempts) before it reaches the internal network. This helps to protect against cyberattacks such as Distributed Denial of Service (DDoS), man-in-the-middle attacks, and brute force attacks.

```
chanuli@server:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.56.103       anywhere             tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootps
ACCEPT     udp  --  anywhere             anywhere             udp spt:bootps dpt:bootpc
ACCEPT     tcp  --  server.example.com   anywhere             tcp dpt:9100
DROP       tcp  --  anywhere             anywhere             tcp dpt:9100

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  anywhere             anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ACCEPT     tcp  --  anywhere             anywhere             tcp spt:https
ACCEPT     udp  --  anywhere             anywhere             udp dpt:bootpc
```

3) Enable Network Time Protocol (NTP)

NTP ensures that the machine's time is synchronized with trusted NTP servers. Accurate time is crucial for logging, security audits, and time-sensitive protocols like Kerberos.

- Accurate Timekeeping for Logs and Audits: Precise time synchronization is essential for tracking security incidents, correlating logs across multiple systems, and conducting forensic analysis. NTP ensures that all devices on a network have consistent timestamps for logging and auditing, which is critical for detecting and responding to breaches

```
chanuli@server:~$ timedatectl status
               Local time: Tue 2024-10-01 03:26:12 +0530
           Universal time: Mon 2024-09-30 21:56:12 UTC
                 RTC time: Mon 2024-09-30 21:56:12
                Time zone: Asia/Colombo (+0530, +0530)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

4) Use secure file permission

Using secure file permissions is crucial for several reasons especially if you have sensitive data and it helps to maintain system integrity. These are some reasons why secure file permission is needed.

- Prevent Unauthorized Access: By setting the correct permissions, can ensure that only authorized users (owners or specific groups) can access, modify, or execute files. This prevents unauthorized users from viewing or editing with sensitive files.
- Protect Sensitive Data: Files containing personal information, financial records, or confidential business data must be protected. Incorrect file permissions can expose this data to unauthorized users, increasing the risk of data breaches.
- Limit System Vulnerabilities: Improperly set permissions can allow attackers to exploit files or directories to inject malicious code, leading to system compromises.
- Ensure System Integrity: Secure file permissions prevent accidental modifications or deletions by limiting the access rights. This is important for system files, configuration files, and software binaries to ensure that they are not modified, which could break system functionality.

Command ‘chmod’ is used to change file permission.

I changed this localhost.key file permission to only owner can read, write and execute that file.

```
-rw----r--  1 chanuli chanuli  1704 Sep 29 01:47 localhost.key
```

```
chanuli@server:~$ chmod 700 localhost.key
```

```
-rwx------  1 chanuli chanuli  1704 Sep 29 01:47 localhost.key
```

5) Back-up configuration

- Protection Against Ransomware: Ransomware attacks encrypt data and demand payment for its release. Having an up-to-date backup allows you to restore your system without paying the ransom, minimizing the impact of the attack.
- Mitigating Insider Threats: Backups protect against malicious insiders or employees accidentally deleting or modifying important data. You can restore the affected systems and data from backups.
- Data Integrity: Regular backups ensure that data remains consistent and unaltered. This helps to detect unauthorized changes or corruption of critical data, ensuring integrity.
- Recovery from Cyber-Attacks: Cyber-attacks can lead to data loss or corruption. Having a backup allows for swift recovery and minimizes downtime, ensuring that critical systems are back online quickly.

In my home directory there is file called ‘localhost.key’. The command ‘cp’ using I make a copy of that file to ‘snp’ directory. If I accidently lost ‘localhost.key’ file there is a backup file in ‘snp’ directory.

```
chanuli@server:~$ pwd
/home/chanuli
```

```
chanuli@server:~$ ls
backup   Documents  localhost.key  Pictures  snap  system_reports  Videos
Desktop  Downloads  Music          Public    snp   Templates
chanuli@server:~$ cd snp
chanuli@server:~/snp$ pwd
/home/chanuli/snp
```

```
chanuli@server:~$ cd snp
chanuli@server:~/snp$ ls
snp1.txt
```

```
chanuli@server:~$ cp localhost.key /home/chanuli/snp
chanuli@server:~$ cd snp
chanuli@server:~/snp$ ls
localhost.key  snp1.txt
```

6) Regularly Review Logs

Network interfaces and services often leave traces in system logs (/var/log/). Reviewing logs can reveal unauthorized access attempts, network issues, or configuration errors.

- Detecting Anomalies: Log files can provide detailed records of network activity. By regularly reviewing these logs, unusual patterns or unauthorized access attempts can be identified early, such as failed login attempts, unexpected spikes in traffic, or communication with unknown IP addresses.

- Incident Response: Logs play a critical role in responding to security incidents. They can provide crucial evidence of how an attack happened, what systems were affected, and the scope of the breach. Without regular review, important warning signs may be missed, allowing a threat to persist unnoticed.

```
chanuli@server:~$ sudo tail -f /var/log/syslog
[sudo] password for chanuli:
2024-10-02T02:37:53.278245+05:30 server gnome-shell[2387]: GFileInfo created without standard::icon
2024-10-02T02:37:53.278435+05:30 server gnome-shell[2387]: file ../../../gio/gfileinfo.c: line 1765 (g_file_info_get_icon): shou
ld not be reached
2024-10-02T02:37:56.247401+05:30 server NetworkManager[788]: <info>  [1727816876.2455] dhcp4 (enp0s8): state changed new lease,
address=192.168.56.102
2024-10-02T02:37:56.248693+05:30 server dbus-daemon[640]: [system] Activating via systemd: service name='org.freedesktop.nm_disp
atcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.11' (uid=0 pid=788 comm="/usr/sbin/NetworkManager --n
o-daemon" label="unconfined")
2024-10-02T02:37:56.264195+05:30 server systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatch
er Service...
2024-10-02T02:37:56.275314+05:30 server dbus-daemon[640]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher
'
2024-10-02T02:37:56.275462+05:30 server systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatche
r Service.
2024-10-02T02:38:06.292803+05:30 server systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
2024-10-02T02:38:15.375779+05:30 server systemd[1]: fprintd.service: Deactivated successfully.
2024-10-02T02:38:42.818501+05:30 server systemd[2139]: Started vte-spawn-dd9abf17-d1e6-480c-b4ad-74771ea47b68.scope - VTE child
process 4132 launched by gnome-terminal-server process 3314.
```

```
chanuli@server:~$ sudo grep "Failed password" /var/log/auth.log
[sudo] password for chanuli:
2024-10-02T02:17:02.578536+05:30 server sudo:  chanuli : TTY=pts/0 ; PWD=/home/chanuli ; USER=root ; COMMAND=/usr/bin/grep 'Fail
ed password' /var/log/auth.log
2024-10-02T02:41:15.770598+05:30 server sudo:  chanuli : TTY=pts/0 ; PWD=/home/chanuli ; USER=root ; COMMAND=/usr/bin/grep 'Fail
ed password' /var/log/auth.log
```