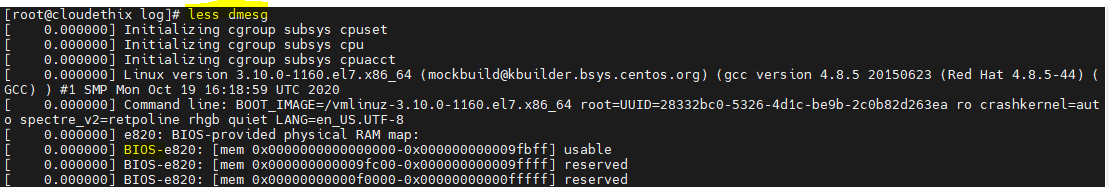
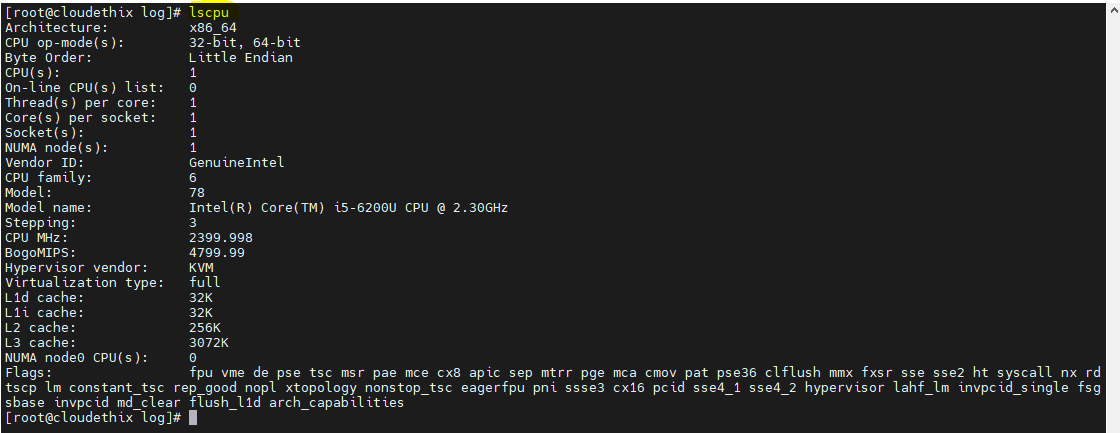
**Question1**- System Logs and Monitoring: user-level & group-level permissions . \* Demonstrate about system logs and monitoring (e.g., dmesg, journalctl, dmidecode, biosdecode, lscpu, free)

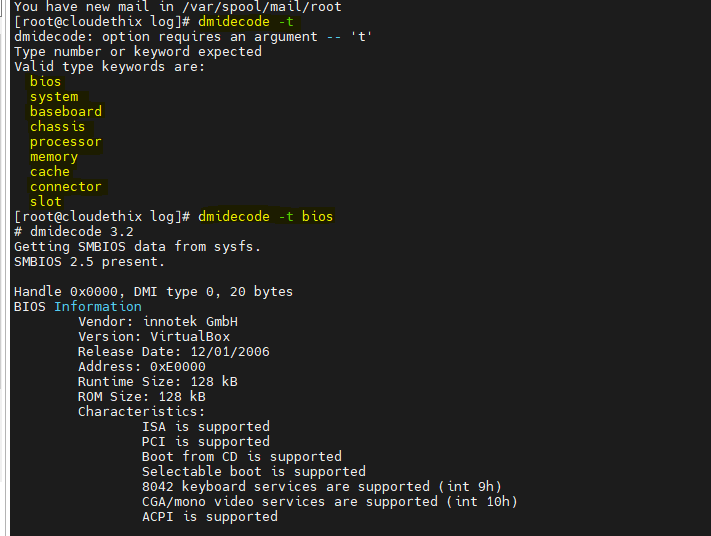
**Dmesg-** this file contains the stores information about **hardware, device driver** of the linux system.



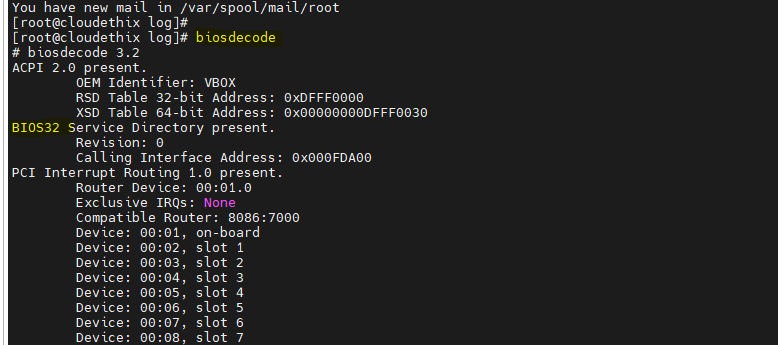
**Lscpu-** this command used to display to get CPU information of the system.



**Dmidecode-** Dmidecodes stands for Desktop Management Interface table decoder. when the user want to retrieve system's hardware related information such as Processor, RAM(DIMMs), BIOS detail, Memory, Serial numbers etc.

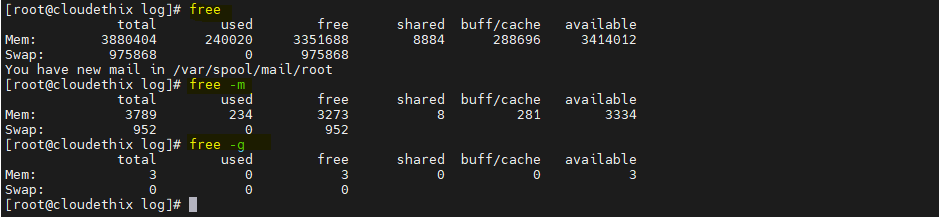


**Biosdecode-** this command is shows the details of the bios setup.

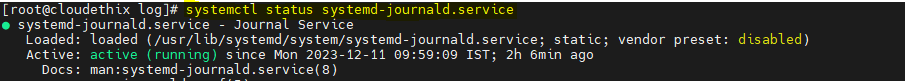


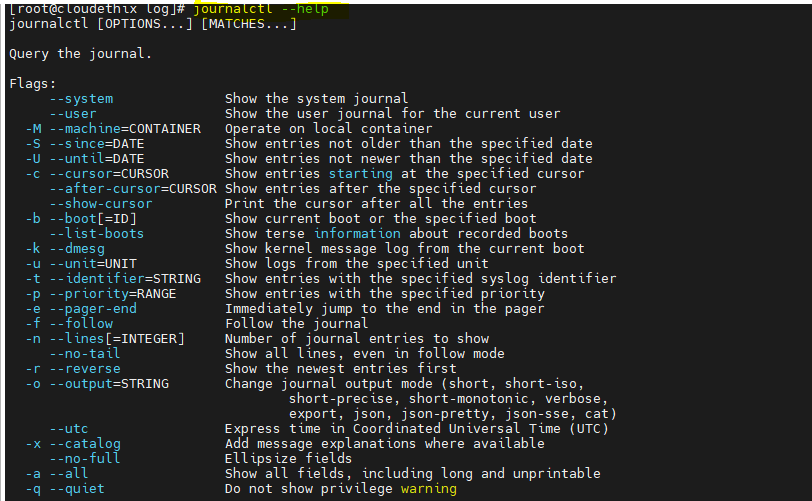
**Free-** this command showing the memory of the system.

If you using flag –m=MB(shows size in mb), -g=GB(shows in gb)



**Journalctl**-The journalctl command is a utility that allows users to view and interact with systemd journal logs. These logs include information from various sources, such as the kernel, system services, applications, and **systemd** itself.





**Question2**. Service Configuration and Management:

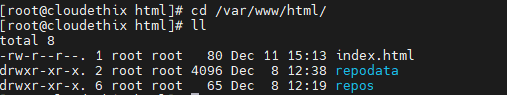
\* Configure and manage services \* Use default httpd & nginx (e.g., systemctl and service ). Use default index.html as the home page, change the default document root of HTTP .

Service= A linux service is an application that runs in the background waiting to be execute. Or carrying essential task.

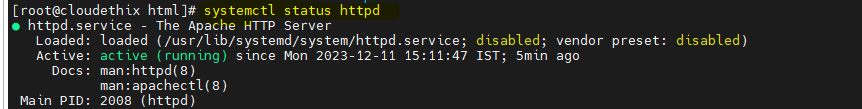
yum install httpd –y

GO to the /var/www/html/ and create one HTML file

vi.index.html



after that start httpd service.



Copy your ip address by using ifconfig command and paste into web browser.

Web page deploy successfully.



**Question3-** User and Group Management:

\* Demonstrate about users and groups (e.g., adduser, usermod, groupadd, and groupmod ).

\* Create multiple users & groups .

\* Add users to multiple groups & modify the user-level & group-level permissions.

Two main Read file :-

/etc/login.defs

/etc/default/useradd

4 database files in linux.

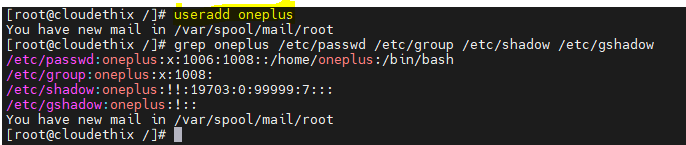
/etc/passwd

/etc/group

/etc/shadow

/etc/gshadow

Adduser: useradd user\_name



Groupadd: groupadd group\_name



Usermod: usermod means user modification

usermod –a \_G group\_name user\_name







Groupmod: **groupmod** command in Linux is used to modify or change the existing group on Linux system.





Task : add user Vicky to grp A

Add user tushar to grp B



Add users to multiple groups:

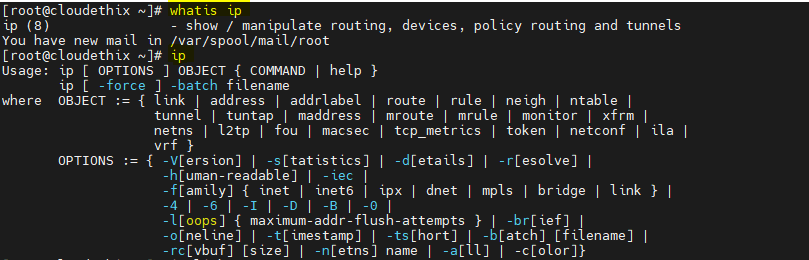




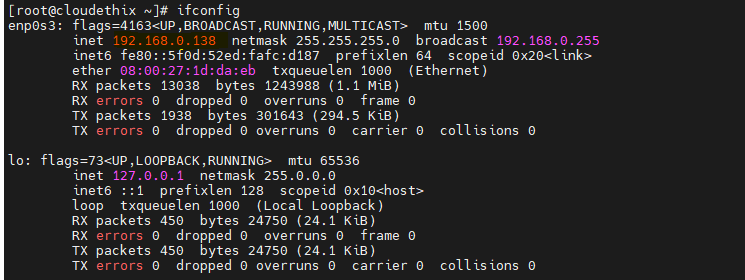
**Question 4-** Networking Basics:

\* Explore networking basics (e.g., ip, ifconfig, ping, traceroute, and netstat )

Ip: IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels. The ip command is straightforward to use, but it includes many complex options. It is not possible to use the ip command by itself. One of the “ip objects” must also be included.

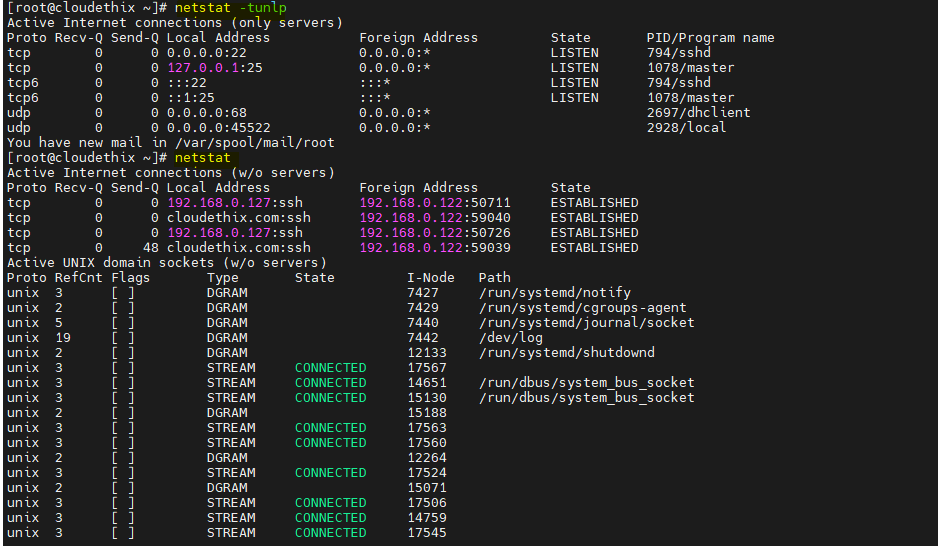


Ifconfig : The command ifconfig stands for interface configurator. The ifconfig command must be used at system startup to define the network address of each interface present on a system.

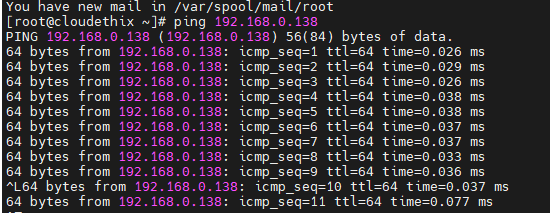


Netstat : The network statistics ( netstat ) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.

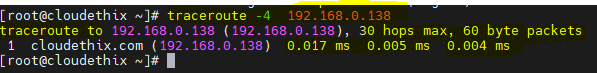
Linux netstat command stands for **Network statistics**. It displays information about different interface statistics, including open sockets, routing tables, and connection information. Further, it can be used to displays all the socket connections (including TCP, UDP).



Ping: The ping command in Linux is a utility that helps to test connectivity between two devices on a network. ping command sends a request to a specified device and waits for a response. response from device helps us to determine whether device is available or not.



Traceroute : The “traceroute” command is a network diagnostic tool that allows users to track the route that a packet takes from the source computer to the destination.



**Question 5-** SSH Server and Key-Based Authentication:

\* Set up an SSH server and learn to use key-based authentication .

\* Force password-based authentication.

\* Check the SSH logs

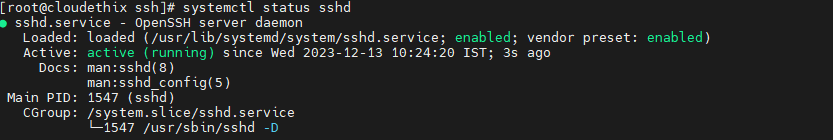
SSH:- Secure socket host (port 22)

SSH is a widely used network protocol that provides a secure way to access remote servers and computers.

The main configuration file of the SSH server is located at "/etc/ssh/sshd\_config".

[root@cloudethix ssh]# yum install openssh-server -y

[root@cloudethix ssh]# systemctl start sshd



key-based authentication .

**Password less authentication:**

First you need to create a keygen.

[root@cloudethix ~]# **ssh-keygen**

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

Created directory '/root/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa.

Your public key has been saved in /root/.ssh/id\_rsa.pub.

The key fingerprint is:

SHA256:PdAkUXXy/FQOYh1ReVvcuwvmm+mIw/30fqSRmPPSNRg root@cloudethix.com

The key's randomart image is:

+---[RSA 2048]----+

| ooo.=.===|

| + . \*.+\*|

| . . o B|

| o E = |

| S o oo.o|

| .++ooo|

| . . o=.=o|

| o..+.B..|

| ...oBoo.|

+----[SHA256]-----+

You have new mail in /var/spool/mail/root

[root@cloudethix ~]# cd /root/.ssh/

You have new mail in /var/spool/mail/root

[root@cloudethix .ssh]# ll

total 8

-rw-------. 1 root root 1675 Dec 13 14:28 **id\_rsa-------------------------------private key**

-rw-r--r--. 1 root root 401 Dec 13 14:28 **id\_rsa.pub-------------------------public key**

You need to add public key to remote machine.

[root@cloudethix .ssh]# ssh-copy-id -i id\_rsa.pub [root@192.168.0.129](mailto:root@192.168.0.129)

After that you are login to the remote machine

**[root@cloudethix .ssh]# ssh root@192.168.0.129**

**Last login: Wed Dec 13 14:21:22 2023 from 192.168.0.119**

It will be login successfully without asking password of the remote machine.

**Force password-based authentication:**

**First create one user on machine ec2-user.**

[root@cloudethix ~]# adduser ec2-user

You have new mail in /var/spool/mail/root

[root@cloudethix ~]# passwd ec2-user

**Changing password for user ec2-user.**

New password:

BAD PASSWORD: The password contains the user name in some form

Retype new password:

passwd: all authentication tokens updated successfully.

**After that allow super-user privileges to ec2-user**

**Go to visudo file and gives full privileges ec2-user ALL=(ALL) ALL**

**Login to ec2-user for ssh-keygen.**

[root@cloudethix ~]# su - ec2-user

[ec2-user@cloudethix ~]$ ls -la

total 12

drwx------. 2 ec2-user ec2-user 62 Dec 13 22:43 .

drwxr-xr-x. 13 root root 174 Dec 13 22:43 ..

-rw-r--r--. 1 ec2-user ec2-user 18 Apr 1 2020 .bash\_logout

-rw-r--r--. 1 ec2-user ec2-user 193 Apr 1 2020 .bash\_profile

-rw-r--r--. 1 ec2-user ec2-user 231 Apr 1 2020 .bashrc

[ec2-user@cloudethix ~]$ ssh-keygen

**Generating public/private rsa key pair.**

**Enter file in which to save the key (/home/ec2-user/.ssh/id\_rsa):**

Created directory '/home/ec2-user/.ssh'.

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /home/ec2-user/.ssh/id\_rsa.

Your public key has been saved in /home/ec2-user/.ssh/id\_rsa.pub.

The key fingerprint is:

SHA256:JxB+dvlkHvSGv63EG/qV3NXmvTtG2iS4a5OriVYsIUM ec2-user@cloudethix.com

The key's randomart image is:

+---[RSA 2048]----+

| . . |

| E . o o |

| . o o o = o |

| o = . = + .|

| o S . + . +|

| . = . o.B=|

| o o @o\*|

| .. .= + O.|

| .. ooo=.=oo|

+----[SHA256]-----+

**Logout the ec2-user and go to the ssh service config file. /etc/ssh/sshd\_config**

**Vi /etc/ssh/sshd\_config**

**Disable the passwordAuthentication NO and enable the pubkeyAuthentication YES**

**Restart the sshd service [root@cloudethix ssh]# systemctl restart sshd**

**After that you have to go to the [root@cloudethix ssh]# cd /home/ec2-user/**

**Copy all the data from id\_rsa file and save as a .pem extension on desktop.**

**Go to puttygen—load---select .pem file---load----save as .ppk file**

**After that go to putty provide ip and select AUTH browse .ppk file.**

**Then create one authorised key file in /home/ec2-user with rsa.pub file.**

[root@cloudethix .ssh]# cat id\_rsa.pub >authorized\_keys

**Change ownership and permission of authorized\_keys**

[root@cloudethix .ssh]# chown ec2-user:ec2-user authorized\_keys

You have new mail in /var/spool/mail/root

[root@cloudethix .ssh]# ll

total 12

-rw-------. 1 ec2-user ec2-user 405 Dec 13 23:22 authorized\_keys

-rw-------. 1 ec2-user ec2-user 1679 Dec 13 22:50 id\_rsa

-rw-r--r--. 1 ec2-user ec2-user 405 Dec 13 22:50 id\_rsa.pub

**After this task complete you have to login without password.**

login as: ec2-user

Authenticating with public key "imported-openssh-key"

Last login: Wed Dec 13 22:49:21 2023

[ec2-user@cloudethix ~]$

SSH LOG:  SSH logs are located at "**/var/log/secure**"

**Question 6-**DNS Tools:

\* Demonstrate the use of DNS tools (e.g., dig and nslookup)

**Dig**: command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems.

**It will show some records:**

A-Address (IPV4)

AAAA-points to IPv6 address of machine

MX – points to email servers

CNAME – canonical name

NS – nameservers for subdomains

PTR – IP address to hostname

SOA Authoritative information about a DNS zone

[root@cloudethix ~]# **dig google.com**

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7\_9.15 <<>> google.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10782

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;google.com. IN A

;; ANSWER SECTION:

google.com. 182 IN A 142.250.183.110

;; AUTHORITY SECTION:

google.com. 95542 IN NS ns2.google.com.

google.com. 95542 IN NS ns4.google.com.

google.com. 95542 IN NS ns1.google.com.

google.com. 95542 IN NS ns3.google.com.

;; ADDITIONAL SECTION:

ns2.google.com. 268967 IN A 216.239.34.10

ns2.google.com. 270257 IN AAAA 2001:4860:4802:34::a

ns3.google.com. 269800 IN A 216.239.36.10

ns3.google.com. 281270 IN AAAA 2001:4860:4802:36::a

ns4.google.com. 271053 IN A 216.239.38.10

ns4.google.com. 279996 IN AAAA 2001:4860:4802:38::a

ns1.google.com. 269024 IN A 216.239.32.10

ns1.google.com. 270257 IN AAAA 2001:4860:4802:32::a

;; Query time: 39 msec

;; SERVER: 192.168.0.1#53(192.168.0.1)

;; WHEN: Thu Dec 14 11:02:52 IST 2023

;; MSG SIZE rcvd: 303

**Nslookup**: Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server.

[root@cloudethix ~]# nslookup google.com

Server: 192.168.0.1

Address: 192.168.0.1#53

Non-authoritative answer:

Name: google.com

Address: 142.250.183.110

Name: google.com

Address: 2404:6800:4009:823::200e

**Question 7-** Cron Job Scheduling System:

\* Familiarize yourself with the cron job scheduling system & set up 5 cron jobs.

\* Check the cron logs

Crontab is a time-based job scheduler. It allows users to schedule jobs (commands or scripts) to run periodically at fixed times, dates, or intervals.

The crontab contains the five star syntax (\*)

Minute (0 - 59)

Hour (0 - 23)

Day of the month (1 - 31)

Month (1 - 12)

Day of the week (0 - 6, where Sunday is 0 or 7)

The system-wide crontab is usually located in **/etc/crontab.**

Options:

-u <user> define user

**-e** edit user's crontab

**-l** list user's crontab

**-r** delete user's crontab

-i prompt before deleting

-n <host> set host in cluster to run users' crontabs

-c get host in cluster to run users' crontabs

-s selinux context

-x <mask> enable debugging

Set the crontab in cron –e file

[root@cloudethix etc]# crontab -l

#At every 30th minute.

\*/30 \* \* \* \* command.sh

#At 09:45 on Sunday.

45 9 \* \* SUN command.sh

#At every 5th minute.

\*/5 \* \* \* \* command.sh

#At 08:00 everyday.

0 8 \* \* \* command.sh

**The file located in cd /var/spool/cron/**

**Question 8-** Disk and Partition Management:

\* Learn about disk and partition management ( eg. fdisk, parted, and df ).

\*Create partitions for each file system.

[root@cloudethix ~]# **fdisk -l**

Disk /dev/sda: 8589 MB, 8589934592 bytes, 16777216 sectors

Units = sectors of 1 \* 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk label type: dos

Disk identifier: 0x000e07f7

Device Boot Start End Blocks Id System

/dev/sda1 \* 2048 976895 487424 83 Linux

/dev/sda2 976896 6836223 2929664 83 Linux

/dev/sda3 6836224 10741759 1952768 83 Linux

/dev/sda4 10741760 16777215 3017728 5 Extended

/dev/sda5 10743808 14649343 1952768 83 Linux

/dev/sda6 14651392 16603135 975872 82 Linux swap / Solaris

Disk /dev/sdb: 8589 MB, 8589934592 bytes, 16777216 sectors

Units = sectors of 1 \* 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk label type: dos

Disk identifier: 0xd2d7875c

Device Boot Start End Blocks Id System

/dev/sdb1 2048 8390655 4194304 83 Linux

/dev/sdb2 8390656 16777215 4193280 83 Linux

Disk /dev/sdc: 16.4 GB, 16375521280 bytes, 31983440 sectors

Units = sectors of 1 \* 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 512 bytes

I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk label type: dos

Disk identifier: 0x6fc654bd

Device Boot Start End Blocks Id System

/dev/sdc1 2048 31983439 15990696 83 Linux

[root@cloudethix ~]# **df -h**

Filesystem Size Used Avail Use% Mounted on

devtmpfs 1.9G 0 1.9G 0% /dev

tmpfs 1.9G 0 1.9G 0% /dev/shm

tmpfs 1.9G 8.7M 1.9G 1% /run

tmpfs 1.9G 0 1.9G 0% /sys/fs/cgroup

/dev/sda2 2.8G 2.3G 536M 82% /

/dev/sdb2 4.0G 33M 4.0G 1% /data02

/dev/sdb1 4.0G 33M 4.0G 1% /data01

/dev/sda3 1.9G 39M 1.9G 3% /home

/dev/sda1 473M 134M 340M 29% /boot

/dev/sda5 1.9G 370M 1.5G 20% /var

/dev/sdc1 16G 13G 2.4G 85% /var/www/html

tmpfs 379M 0 379M 0% /run/user/0

**Question 9-** File Systems and Mounting:

Explore file systems and mounting (e.g., ext2, ext3, ext4, xfs, and nfs ).

Format partitions accordingly with the file system.

[root@vivek ~]# **cat /etc/fstab**

# /etc/fstab

# Created by anaconda on Thu Dec 7 21:10:11 2023

# Accessible filesystems, by reference, are maintained under '/dev/disk'

# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info

/dev/sdb1 /data01 xfs defaults 0 0

/dev/sdb2 /data02 xfs defaults 0 0

/dev/sdc1 /data1 **ext2**  defaults 0 0

/dev/sdc2 /data2 **ext3**  defaults 0 0

/dev/sdc3 /data3 **ext4**  defaults 0 0

/dev/sdc5 /data5 **xfs** defaults 0 0

[root@vivek ~]# **df -h**

Filesystem Size Used Avail Use% Mounted on

devtmpfs 1.9G 0 1.9G 0% /dev

tmpfs 1.9G 0 1.9G 0% /dev/shm

tmpfs 1.9G 8.7M 1.9G 1% /run

tmpfs 1.9G 0 1.9G 0% /sys/fs/cgroup

/dev/sda2 2.8G 1.2G 1.7G 43% /

/dev/sda3 1.9G 33M 1.9G 2% /home

/dev/sdb1 4.0G 33M 4.0G 1% /data01

/dev/sdb2 4.0G 33M 4.0G 1% /data02

/dev/sda1 473M 134M 340M 29% /boot

/dev/sda5 1.9G 340M 1.6G 18% /var

tmpfs 379M 0 379M 0% /run/user/0

/dev/sdc1 2.0G 3.0M 1.9G 1% /root/data1

/dev/sdc2 2.0G 3.1M 1.9G 1% /root/data2

/dev/sdc3 2.0G 6.0M 1.8G 1% /root/data3

/dev/sdc5 2.0G 33M 2.0G 2% /root/data5

**Question 10-** LAMP Stack:

\* Set up a basic LAMP ( Linux, Apache, MySQL, PHP ) stack.

Installation of Apache (http): port 80

[root@cloudethix ~]# **yum install httpd -y**

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

\* base: bd.mirror.vanehost.com

\* extras: mirrors.hostever.com

\* updates: bd.mirror.vanehost.com

base | 3.6 kB 00:00:00

extras | 2.9 kB 00:00:00

updates | 2.9 kB 00:00:00

Package httpd-2.4.6-99.el7.centos.1.x86\_64 already installed and latest version

Nothing to do

[root@cloudethix ~]# **systemctl start httpd**

[root@cloudethix ~]# **systemctl status httpd**

● httpd.service - The Apache HTTP Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)

Active: active (running) since Sat 2023-12-16 13:12:15 IST; 7s ago

Docs: man:httpd(8)

man:apachectl(8)

Main PID: 1421 (httpd)

Status: "Processing requests..."

CGroup: /system.slice/httpd.service

├─1421 /usr/sbin/httpd -DFOREGROUND

├─1422 /usr/sbin/httpd -DFOREGROUND

├─1423 /usr/sbin/httpd -DFOREGROUND

├─1424 /usr/sbin/httpd -DFOREGROUND

├─1425 /usr/sbin/httpd -DFOREGROUND

└─1426 /usr/sbin/httpd -DFOREGROUND

[root@cloudethix ~]# **netstat -tunlp**

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 797/sshd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 1068/master

tcp6 0 0 :::**80** :::\* LISTEN 1421/httpd

tcp6 0 0 :::22 :::\* LISTEN 797/sshd

tcp6 0 0 ::1:25 :::\* LISTEN 1068/master

udp 0 0 0.0.0.0:68 0.0.0.0:\* 617/dhclient

**Installation of MYSQL:**

[root@cloudethix ~]# **yum install mysql -y**

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

\* base: centos.mirror.net.in

\* extras: centos.mirror.net.in

\* updates: centos.mirror.net.in

Resolving Dependencies

--> Running transaction check

---> Package mariadb.x86\_64 1:5.5.68-1.el7 will be installed

--> Finished Dependency Resolution

Dependencies Resolved

=========================================================================================================================================

Package Arch Version Repository Size

=========================================================================================================================================

Installing:

mariadb x86\_64 1:5.5.68-1.el7 base 8.8 M

Transaction Summary

=========================================================================================================================================

Install 1 Package

Total download size: 8.8 M

Installed size: 49 M

Downloading packages:

mariadb-5.5.68-1.el7.x86\_64.rpm | 8.8 MB 00:00:04

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Installing : 1:mariadb-5.5.68-1.el7.x86\_64 1/1

Verifying : 1:mariadb-5.5.68-1.el7.x86\_64 1/1

Installed:

mariadb.x86\_64 1:5.5.68-1.el7

Complete!

**Installation of PHP:**

[root@cloudethix ~]# yum install php -y

Loaded plugins: fastestmirror

Loading mirror speeds from cached hostfile

\* base: bd.mirror.vanehost.com

\* extras: mirrors.hostever.com

\* updates: bd.mirror.vanehost.com

Resolving Dependencies

--> Running transaction check

---> Package php.x86\_64 0:5.4.16-48.el7 will be installed

--> Processing Dependency: php-common(x86-64) = 5.4.16-48.el7 for package: php-5.4.16-48.el7.x86\_64

--> Processing Dependency: php-cli(x86-64) = 5.4.16-48.el7 for package: php-5.4.16-48.el7.x86\_64

--> Running transaction check

---> Package php-cli.x86\_64 0:5.4.16-48.el7 will be installed

---> Package php-common.x86\_64 0:5.4.16-48.el7 will be installed

--> Processing Dependency: libzip.so.2()(64bit) for package: php-common-5.4.16-48.el7.x86\_64

--> Running transaction check

---> Package libzip.x86\_64 0:0.10.1-8.el7 will be installed

--> Finished Dependency Resolution

Dependencies Resolved

=========================================================================================================================================

Package Arch Version Repository Size

=========================================================================================================================================

Installing:

php x86\_64 5.4.16-48.el7 base 1.4 M

Installing for dependencies:

libzip x86\_64 0.10.1-8.el7 base 48 k

php-cli x86\_64 5.4.16-48.el7 base 2.7 M

php-common x86\_64 5.4.16-48.el7 base 565 k

Transaction Summary

=========================================================================================================================================

Install 1 Package (+3 Dependent packages)

Total download size: 4.7 M

Installed size: 17 M

Downloading packages:

(1/4): libzip-0.10.1-8.el7.x86\_64.rpm | 48 kB 00:00:00

(2/4): php-5.4.16-48.el7.x86\_64.rpm | 1.4 MB 00:00:01

(3/4): php-common-5.4.16-48.el7.x86\_64.rpm | 565 kB 00:00:00

(4/4): php-cli-5.4.16-48.el7.x86\_64.rpm | 2.7 MB 00:00:00

-----------------------------------------------------------------------------------------------------------------------------------------

Total 2.2 MB/s | 4.7 MB 00:00:02

Running transaction check

Running transaction test

Transaction test succeeded

Running transaction

Warning: RPMDB altered outside of yum.

Installing : libzip-0.10.1-8.el7.x86\_64 1/4

Installing : php-common-5.4.16-48.el7.x86\_64 2/4

Installing : php-cli-5.4.16-48.el7.x86\_64 3/4

Installing : php-5.4.16-48.el7.x86\_64 4/4

Verifying : php-5.4.16-48.el7.x86\_64 1/4

Verifying : libzip-0.10.1-8.el7.x86\_64 2/4

Verifying : php-cli-5.4.16-48.el7.x86\_64 3/4

Verifying : php-common-5.4.16-48.el7.x86\_64 4/4

Installed:

php.x86\_64 0:5.4.16-48.el7

Dependency Installed:

libzip.x86\_64 0:0.10.1-8.el7 php-cli.x86\_64 0:5.4.16-48.el7 php-common.x86\_64 0:5.4.16-48.el7

Complete!