Advanced Linux
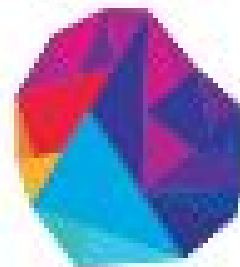
1. **What is the size of MBR and what does it contains.**

MBR stands for Master Boot Record. Most legacy disks are MBR disks. MBR disks store partition information in the MBR, hence the name. This information is generally stored in the first sector of the disk.The total size of the MBR is 512 bytes, which contains the bootloader program and disk partitioning information.
- 446 bytes bootloader
- 64(4*16bytes) Partition Table
- 2 bytes magic no.

2. **In which file you can write commands which you want to run whenever Linux system starts/restarts?**

In this method, we will use 'rc.local' file located in '/etc/' to execute our scripts and commands at startup. We will make an entry to execute the script in the file & every time when our system starts, the script will be executed.

But we will first provide the permissions to make the file /etc/rc.local executable,

$ sudo chmod +x /etc/rc.local

Next we will add the script to be executed in the file,

3. **Reboot the system using runlevel.**

ANS : Use command $ init 6

4. **Restart cron service**

ANS:To restart cron service, enter: $`sudo /etc/init.d/cron restart`
Or $ `sudo service cron restart`

5. **Create an ext4 filesystem**

Ans : We can create using :
        Mkfs.ext4 /dev/sdb1

6. Mount the created filesystem on /partition directory.

Ans: To attach a partition or device, mount point must be created. A mount point is simply a directory created with mkdir, then attach a partition by using mount.

    mkdir test
    Mount /dev/sda1 /test

7. Difference between LVM and RAID.

S.No.	RAID	LVM
1.	RAID is used for redundancy.	LVM is a way in which you partition the hard disk logically and it contains its own advantages.
2.	A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.	LVM is a logical layer that that can be anipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
3.	RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.	LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc

4.	RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.	LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.
5.	RAID is NOT any kind of Data backup solution. Its a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.	LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.

8. Create a LVM(Slide 13)

```
diksha@diksha:~$ sudo apt-get install lvm2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dmeventd libdevmapper-event1.02.1 liblvm2app2.2 liblvm2cmd2.02 libreadline5
Suggested packages:
  thin-provisioning-tools
The following NEW packages will be installed:
  dmeventd libdevmapper-event1.02.1 liblvm2app2.2 liblvm2cmd2.02 libreadline5
  lvm2
```

- Select the Physical Storage Devices for LVM – Use pvcreate, pvscan, pvdisplay Commands

  `pvcreate /dev/sda6 /dev/sda7`
- Create the Volume Group – Use vgcreate, vgdisplay

Commands

```
vgcreate vol_grp1 /dev/sda6 /dev/sda7
```

- LVM deals with extents as Physical volumes deals with blocks.
- LVM Create: Create Logical Volumes – Use lvcreate, lvdisplay command

```
lvcreate -l 20 -n logical_vol1 vol_grp1
```

- Formatting lv: `mkfs.ext3 /dev/vol_grp1/logical_vol1`

9. Create a RAID1 device(Slide 19)

```
diksha@diksha:~$ sudo  apt-get install mdadm rsync initramfs-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
rsync is already the newest version (3.1.2-2.1ubuntu1).
The following additional packages will be installed:
  initramfs-tools-bin initramfs-tools-core
Suggested packages:
  default-mta | mail-transport-agent dracut-core
The following NEW packages will be installed:
  mdadm
The following packages will be upgraded:
  initramfs-tools initramfs-tools-bin initramfs-tools-core
3 upgraded, 1 newly installed, 0 to remove and 621 not upgraded.
Need to get 416 kB/484 kB of archives.
After this operation, 1,246 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Setup RAID:

- **Installation**: apt-get install mdadm rsync initramfs-tools
- **Create partitions** on these two drives using 'fdisk' command say /dev/sdb and /dev/sdc
- **Verify the changes** on both sdb & sdc
  #mdadm -E /dev/sd[b-c]
- **Create RAID1 Device** called '/dev/md0'
  #mdadm --create /dev/md0 --level=mirror --raid-devices=2 /dev/sd[b-c]1
  #cat /proc/mdstat
- **Check the raid devices type**:
  #mdadm -E /dev/sd[b-c]1
  #mdadm --detail /dev/md0
- **Create file system** using ext4 for md0 and mount under /mnt/raid1

```
#mkfs.ext4 /dev/md0
#mkdir /mnt/raid1
#mount /dev/md0 /mnt/raid1/
```

10.   Create a swapfile of 500Mb(slide20)

Swap : OS temporarily stores data that it can no longer hold in RAM.

```
1)Check swap:
#sudo swapon -s
#free -m
2)Check current disk usage:
#df -h
3)Create a Swap File:
Traditional and Slow Way:
        #sudo dd if=/dev/zero of=/swapfile bs=1G count=4
        #ls -lh /swapfile
            -rw-r--r-- 1 root root 4.0G Apr 28 17:15 /swapfile
Faster Way: creates a file of a preallocated size instantly, without
actually having to write dummy contents
        #sudo fallocate -l 4G /swapfile
4)Set up the swap space:
#sudo mkswap /swapfile
5)Enable swap space:
#sudo swapon /swapfile
6)Verify swap space:
#swapon -s
```

11.   Set setuid and setgid on two different file.

ID	File	Directory
SUID	Run program as owner of the file	-
SGID	Assign authority to run program as owner of the file	Inherit group ownership of all of the item created beneath that directory
Sticky Bit	-	Only owner of the file can delete the file e.g. /tmp

```
diksha@diksha:~$ ls -l a.txt
-rw-r--r-- 1 diksha diksha 6 Feb 12 09:59 a.txt
diksha@diksha:~$ ls -l b.txt
-rw-r--r-- 1 diksha diksha 3 Feb 12 09:59 b.txt
diksha@diksha:~$ chmod u+s a.txt
diksha@diksha:~$ ls -l a.txt
-rwSr--r-- 1 diksha diksha 6 Feb 12 09:59 a.txt
diksha@diksha:~$ chmod g+s b.txt
diksha@diksha:~$ ls -l b.txt
-rw-r-Sr-- 1 diksha diksha 3 Feb 12 09:59 b.txt
diksha@diksha:~$
```

12. What is the use of Sticky bit.

ANS: **Sticky bit** is a user ownership access right flag that can be assigned to files and directories on Unix-like systems.

When a directory's sticky bit is set, the filesystem treats the files in such directories in a special way so only the file's owner, the directory's owner, or root user can rename or delete the file. Without the sticky bit set, any user with write and execute permissions for the directory can rename or

delete contained files, regardless of the file's owner. Typically this is set on the `/tmp` directory to prevent ordinary users from deleting or moving other users' files.

The most common **use** of the sticky bit is on directories residing within filesystems for Unix-like operating systems. When a directory's sticky bit is set, the filesystem treats the files in such directories in a special way so only the file's owner, the directory's owner, or root can rename or delete the file. Without the sticky bit set, any user with write and execute permissions for the directory can rename or delete contained files, regardless of the file's owner.

```
diksha@diksha:~$ ls -l abc.sh
-rw-r--r-- 1 diksha diksha 4 Feb 10 13:08 abc.sh
diksha@diksha:~$ chmod +t abc.sh
diksha@diksha:~$ ls -l abc.sh
-rw-r--r-T 1 diksha diksha 4 Feb 10 13:08 abc.sh
diksha@diksha:~$ chmod o+x abc.sh
diksha@diksha:~$ ls -l abc.sh
-rw-r--r-t 1 diksha diksha 4 Feb 10 13:08 abc.sh
diksha@diksha:~$
```

13. Create a user and add it to one secondary group.

```
diksha@diksha:~$ sudo usermod -a -G diksha test
[sudo] password for diksha:
diksha@diksha:~$ id -a test
uid=1001(test) gid=1001(test) groups=1001(test),0(root),1000(diksha)
diksha@diksha:~$
```

14. Lock this user.

```
diksha@diksha:~$ sudo usermod -L test
diksha@diksha:~$ passwd --status test
passwd: You may not view or modify password information for test.
diksha@diksha:~$ sudo !!
sudo passwd --status test
test L 02/03/2020 0 99999 7 -1
diksha@diksha:~$ █
```

15. Give this user full access (without password).

```
diksha@diksha:~$ sudo passwd -u test
passwd: password expiry information changed.
diksha@diksha:~$ su test
Password:
su: Authentication failure
diksha@diksha:~$ su test
Password:

WELCOME
test@diksha:/home/diksha$ sudo visudo
[sudo] password for test:
test@diksha:/home/diksha$ █
```

```
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:$

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
test    ALL=(ALL) NOPASSWD: ALL
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:


^G Get Help   ^O Write Out ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File ^\ Replace    ^U Uncut Text^T To Spell   ^  Go To Line
```

16. Delete the create user after taking backup of it home directory.

```
test@diksha:~$ sudo tar -cvzf backup.tar.gz /home/test/
tar: Removing leading `/' from member names
/home/test/
/home/test/.bashrc
/home/test/.bash_logout
/home/test/.gnupg/
/home/test/.gnupg/private-keys-v1.d/
/home/test/.dbus/
/home/test/.dbus/session-bus/
/home/test/.dbus/session-bus/56bd8b055f1843d7b33f975ede05e9e5-0
/home/test/.profile
/home/test/.bash_history
/home/test/ball.tar.gz
/home/test/passwd_backup
/home/test/output
```

```
test@diksha:~$ sudo userdel -r test
userdel: user test is currently used by process 8367
test@diksha:~$ kill -9 8367
diksha@diksha:~$ sudo usermod -L test
diksha@diksha:~$
```

17. Create a file with some content. Change all lower case letter to upper case letter and save output to another file using redirections.

```
diksha@diksha:~$ cat >XYZ.txt
heLLO ,hoW ARE you?
diksha@diksha:~$ tr '[:upper:]' '[:lower:]' < input.txt > output.txt
bash: input.txt: No such file or directory
diksha@diksha:~$ tr '[:lower:]' '[:upper:]' <XYZ.txt  >ABCD.txt
diksha@diksha:~$ cat ABCD.txt
HELLO ,HOW ARE YOU?
diksha@diksha:~$
```

```
diksha@diksha:~$ cat >xyz
hey Hello
diksha@diksha:~$ sed -e 's/\(.*\)/\U\1/' xyz > abcd
diksha@diksha:~$ cat abcd
HEY HELLO
diksha@diksha:~$
```

18. Set nice value of a process to -1.

```
diksha@diksha:~$ sudo renice 2 726
726 (process ID) old priority 0, new priority 2
diksha@diksha:~$ top
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
19057	diksha	20	0	838408	167152	95172	S	4.6	1.0	6:54.50	chrome
1250	diksha	19	-1	4251760	554508	79908	S	2.8	3.4	153:11.71	gnome-shell
3639	diksha	20	0	51452	4188	3392	R	1.8	0.0	0:00.19	top

19.Get list of all files used by "telnet".
ANS:

```
diksha@diksha:~$ dpkg -L telnet
/.
/usr
/usr/bin
/usr/bin/telnet.netkit
/usr/share
/usr/share/doc
/usr/share/doc/telnet
/usr/share/doc/telnet/BUGS
/usr/share/doc/telnet/README.gz
/usr/share/doc/telnet/README.telnet
/usr/share/doc/telnet/README.telnet.old.gz
/usr/share/doc/telnet/changelog.Debian.gz
/usr/share/doc/telnet/copyright
/usr/share/lintian
/usr/share/lintian/overrides
/usr/share/lintian/overrides/telnet
/usr/share/man
/usr/share/man/man1
/usr/share/man/man1/telnet.netkit.1.gz
/usr/share/menu
gle Chrome e/menu/telnet
diksha@diksha:~$
```

```
diksha@diksha:~$ dpkg-query -L telnet
/.
/usr
/usr/bin
/usr/bin/telnet.netkit
/usr/share
/usr/share/doc
/usr/share/doc/telnet
/usr/share/doc/telnet/BUGS
/usr/share/doc/telnet/README.gz
/usr/share/doc/telnet/README.telnet
/usr/share/doc/telnet/README.telnet.old.gz
/usr/share/doc/telnet/changelog.Debian.gz
/usr/share/doc/telnet/copyright
/usr/share/lintian
/usr/share/lintian/overrides
/usr/share/lintian/overrides/telnet
/usr/share/man
/usr/share/man/man1
/usr/share/man/man1/telnet.netkit.1.gz
```

20.Check if port 22 is listening using netstat and telnet command.
Netstat command displays various network related information such as
network connections, routing tables, interface statistics, masquerade

connections, multicast memberships etc.,

```
diksha@diksha:~$ netstat -plnt | grep ':22'
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
tcp6       0      0 :::22                   :::*                    LISTEN
-
diksha@diksha:~$
```

```
diksha@diksha:~$ telnet  127.0.0.1 22
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
```

21. Create a cron job which runs once in a week at 23:45
Selection_007
Ans : Type command
    $crontab -e
    45 23 * * 1

22. Difference between dig and traceroute
Dig ([Domain Information Groper](#)) is a command line utility that performs DNS lookup by querying name servers and displaying the result to you.
By default, dig sends the [DNS](#) query to name servers listed in the resolver(/etc/resolv.conf) unless it is asked to query a specific name server.

```
diksha@diksha:~$ dig www.google.com

; <<>> DiG 9.11.3-1ubuntu1.1-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55716
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.google.com.          215      IN      A        172.217.167.196

;; Query time: 18 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Feb 11 17:12:52 IST 2020
;; MSG SIZE  rcvd: 59
```

The output will contain information like the installed dig version, technical details about the answers, statistics about the query, a question section along with few other ones.

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. It will show all of the routers it goes through until it gets to its destination, or it fails.

```
diksha@diksha:~$ traceroute google.com
traceroute to google.com (172.217.167.14), 30 hops max, 60 byte packets
 1  _gateway (10.1.224.1)  5.261 ms  5.238 ms  5.188 ms
 2  nsg-static-185.160.71.182.airtel.in (182.71.160.185)  15.501 ms  15.501 ms *
 3  182.79.149.182 (182.79.149.182)  15.438 ms *  15.438 ms
 4  72.14.217.194 (72.14.217.194)  8.874 ms  8.856 ms  8.859 ms
 5  * * *
 6  209.85.252.44 (209.85.252.44)  20.054 ms  12.839 ms 209.85.251.230 (209.85.2
51.230)  8.990 ms
 7  del03s15-in-f14.1e100.net (172.217.167.14)  12.660 ms * *
diksha@diksha:~$
```