**1)  What is GRUB**

GNU GRUB is a Multiboot boot loader. It is derive from GRUB, the GRand Unified Bootloader,

which was originally designed and implemented by Erich Stefan Boleyn.

Briefly, a boot loader is the first software program that runs when a computer starts. It is

responsible for loading and transferring control to the operating system kernel software

(such as the Hurd or Linux). The kernel, in turn, initializes the rest of the operating

system (e.g. GNU)

**2) Explain Linux Boot Process**

Press the power button on your system, and after few moments, you see the Linux login prompt.

Have you ever wondered what happens behind the scenes from the time you press the power button until the Linux login prompt appears?

The following are the 6 high level stages of a typical Linux boot process.



**a. BIOS**

* BIOS stands for Basic Input/Output System
* Performs some system integrity checks
* Searches, loads, and executes the boot loader program.
* It looks for boot loader in floppy, cd-rom, or hard drive. You can press a key (typically F12 of F2, but it depends on your system) during the BIOS startup to change the boot sequence.
* Once the boot loader program detected and loaded into the memory, BIOS gives the control to it.
* Therefore, in simple terms BIOS loads and executes the MBR boot loader.

**b. MBR**

* MBR stands for Master Boot Record.
* It is located in the 1st sector of the bootable disk. Typically **/dev/hda, or /dev/sda**
* MBR is less than 512 bytes in size. This has three components 1) primary boot loader info in 1st 446 bytes 2) partition table info in next 64 bytes 3) mbr validation check in last 2 bytes.
* It contains information about GRUB (or LILO in old systems).
* So, in simple terms MBR loads and executes the GRUB boot loader.

**c. GRUB**

* **GRUB stands for Grand Unified Bootloader**.
* If you have **multiple kernel images installed on your system**, you can choose which one to execute.
* GRUB displays a splash screen, waits for few seconds, if you do not enter anything; it loads the default kernel image as specified in the grub configuration file.
* GRUB has the knowledge of the filesystem (the **older Linux loader LILO did not understand filesystem**).

Grub configuration file is **/boot/grub/grub.conf (/etc/grub.conf** is a link to this). The following is sample grub.conf of CentOS.

In centos 7 or kernel abv 4, file is /boot/grub2/grub.cfg

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | <span style="background-color: #dff10d; color: #260af4;"><strong>#boot=/dev/sda  default=0  timeout=5  splashimage=(hd0,0)/boot/grub/splash.xpm.gz  hiddenmenu  title CentOS (2.6.18-194.el5PAE)            root (hd0,0)            kernel /boot/vmlinuz-2.6.18-194.el5PAE ro root=LABEL=/            initrd /boot/initrd-2.6.18-194.el5PAE.img</strong></span> |

* As you notice from the above info, it contains kernel and initrd image.
* So, in simple terms GRUB just loads and executes Kernel and initrd images.

**d. Kernel**

* Mounts the root file system as specified in the **“root=” in grub.conf**
* Kernel executes the /sbin/init program
* Since init was the 1st program to be executed by Linux Kernel, it has the **process id (PID)** of 1. Do a **‘ps -ef | grep init’** and check the pid.
* initrd stands for Initial RAM Disk.
* Initrd/initramfs-3.10.0-514.el7.x86\_64.img is used by kernel as temporary root file system until kernel is booted and the real root file system is mounted. It also contains necessary drivers compiled inside, which helps it to access the hard drive partitions, and other hardware.

**e. Init**

* Looks at the /etc/inittab file to decide the Linux run level. Rhel 7>> /etc/system/system/
* Following are the available run levels
  + 0 – halt
  + **1 – Single user mode**
  + **2 – Multiuser, without NFS**
  + **3 – Full multiuser mode**
  + 4 – unused
  + 5 – X11
  + 6 – reboot
* Init identifies the default initlevel from /etc/inittab and uses that to load all appropriate program.
* Execute ‘**grep initdefault** **/etc/inittab**’ on your system to identify the default run level
* If you want to get into trouble, you can set the **default run level** to 0 or 6. Since you know what 0 and 6 means, probably you might not do that.
* Typically you would set the default run level to either 3 or 5.

**f. Runlevel programs**

* When the Linux system is booting up, you might see various services getting started. For example, it might say “starting sendmail …. OK”. Those are the runlevel programs, executed from the run level directory as defined by your run level.
* Depending on your default init level setting, the system will execute the programs from one of the following directories.
  + Run level 0 – /etc/rc.d/rc0.d/
  + **Run level 1 – /etc/rc.d/rc1.d/**
  + **Run level 2 – /etc/rc.d/rc2.d/**
  + **Run level 3 – /etc/rc.d/rc3.d/**
  + **Run level 4 – /etc/rc.d/rc4.d/**
  + Run level 5 – /etc/rc.d/rc5.d/
  + Run level 6 – /etc/rc.d/rc6.d/
* Please note that there are also symbolic links available for these directory under /etc directly. So, /etc/rc0.d is linked to /etc/rc.d/rc0.d.
* Under the /etc/rc.d/rc\*.d/ directories, you would see programs that start with S and K.
* Programs starts with S are used during startup. S for startup.
* Programs starts with K are used during shutdown. K for kill.
* There are numbers right next to S and K in the program names. Those are the sequence number in which the programs should be started or killed.
* For example, S12syslog is to start the syslog deamon, which has the sequence number of 12. S80sendmail is to start the sendmail daemon, which has the sequence number of 80. So, syslog program will be started before sendmail.

There you have it. That is what happens during the Linux boot process.

Change run level in rhel 7:

[root@rhel7 ~]# **systemctl enable graphical.target --force**

rm '/etc/systemd/system/default.target'

ln -s '/usr/lib/systemd/system/graphical.target' '/etc/systemd/system/default.target'

#systemctl get-default

Change default to runlevel 3 (nothing but a multi-user.target).

|  |
| --- |
| # systemctl set-default multi-user.target |

Confirm the default runlevel.

|  |
| --- |
| # systemctl get-default  multi-user.target |

**3) Which files are called for user profile by default when a user gets login**

$HOME/.bash\_profile, **$HOME/.bash\_bashrc**

**4) Which file needs to update if srequired to change default runlevel 5 to 3**

File is **/etc/inittab** and required to change below lines:

**id:5:initdefault: to id:3:initdefault:**

**5) What command used for showing user info like Login Name, Canonical Name, Home Directory,Shell etc..**

**FINGER command can be used i.g; finger username**

**6) What is inode number**

An inode is a data structure on a traditional Unix-style file system such as UFS or ext3. An

**inode stores basic information about a regular file, directory, or other file system object**

iNode number also called as index number, it consists following attributes:

File type (executable, block special etc)

Permissions (read, write etc)

Owner

Group

File Size

File access, change and modification time (remember UNIX or Linux never stores file creation

time, this is favorite question asked in UNIX/Linux sys admin job interview)

File deletion time

Number of links (soft/hard)

Extended attribute such as append only or no one can delete file including root user

(immutability)

Access Control List (ACLs)

Following command will be used to show inodes of file and folders:

ls -i

Following command will show complete info about any file or folders with inode number

stat file/folder

Files/Folders can also be deleted using inode numbers with following command:

find out the inode number using ‘ls -il’ command then run below command

find . -inum inode\_number -exec rm -i {} \;

**7) How can we increase disk read performance in single command**

blockdev command

This is sample output – yours may be different.

# Before test

$ blockdev –getra /dev/sdb

256

$ time dd if=/tmp/disk.iso of=/dev/null bs=256k

2549+1 records in

2549+1 records out

668360704 bytes (668 MB) copied, 6,84256 seconds, 97,7 MB/s

real 0m6.845s

user 0m0.004s

sys 0m0.865s

# After test

$ blockdev –setra 1024 /dev/sdb

$ time dd if=/tmp/disk.iso of=/dev/null bs=256k

2435+1 records in

2435+1 records out

638390272 bytes (638 MB) copied, 0,364251 seconds, 1,8 GB/s

real 0m0.370s

user 0m0.001s

sys 0m0.370s

**8) …. command to change user password expiration time**

CHAGE

**9) Command used to lock user password**

usermod -L username

**10) How many default number of Shells available and what are their names?**

SH, BASH, CSH, TCSH, NOLOGIN, KSH

**11) Which file defines the attributes like UID, PASSWORD expiry, HOME Dir create or not while adding user**

/etc/login.defs

**12) …… command used for changing authentication of linux system to LDAP/NIS/SMB/KERBOS**

authconfig

**13) …… command used for changing the attributes of any file**

chattr

**14) What is the path of network (ethX) configuration files**

/etc/sysconfig/network-scripts/ethX

**15) How can we change speed and make full duplex settings for eth0**

We can do this with below given 2 methods:

ethtool -s eth0 speed 100 duplex full

ethtool -s eth0 speed 10 duplex half

OR

mii-tool -F 100baseTx-HD

mii-tool -F 10baseT-HD

**16) File which stores the DNS configuration at client side**

/etc/resolve.conf

**17) Main configuration file and command used for exporting NFS directories and it’s deamons**

/etc/exports and exportfs -av , deamons are quotad, portmapper, mountd, nfsd and nlockmgr/status

**18) What is command to check ports running/used over local machine**

netstat -antp

**19) What is the command to check open ports at remote machine**

nmap

**20) What is the difference between soft and hard links**

Soft Links => 1) Soft link files will have different inode numbers then source file

2) If original file deleted then soft link file be of no use

3) Soft links are not updated

4) Can create links between directories

5) Can cross file system boundaries

Hard Links => 1) Hard links will have the same inode number as source file

2) Hard links can not link directories

3) Can not cross file system boundaries

4) Hard links always refers to the source, even if moved or removed

**21) How to setup never expired user password**

chage -E never username

22) Restricting insertion into file if full permission are assigned to all

chattr +i filename

**23) Display or Kill all processes which are accessing any folder/file**

Display User who are using file/folder : fuser -u file/folder

Kill All Processes which are using file/folder: fuser -k file/folder

**24) Kill any user’s all processes**

killall -u username

**25) How can we have daily system analysis and reports over mail**

Use logwatch

**26) How can we rotate logs using logrotate without performing any operation  like move and gzip’ng over original file and then creating new file (which is very lengthy process)**

We can use “logrotate”‘s “copytruncate” option which will simply copy original file and truncate original file :)

**27) Command to collect detailed information about the hardware and setup of your system**

dmidecode , sysreport

**28) Command to check PCI devices vendor or version**

Ans lspci

**29) What is the difference between cron and anacron**

Cron :

1) Minimum granularity is minute (i.e Jobs can be scheduled to be executed

every minute)

2) Cron job can be scheduled by any normal user ( if not restricted by super

user )

3) Cron expects system to be running 24 x 7. If a job is scheduled, and

system is down during that time, job is not executed

4) Ideal for servers

5) Use cron when a job has to be executed at a particular hour and minute

Anacron :

1) Minimum granularity is only in days

2) Anacron can be used only by super user ( but there are workarounds to

make it usable by normal user )

3) Anacron doesn’t expect system to be running 24 x 7. If a job is scheduled,

and system is down during that time, it start the jobs when the system

comes back up.

4) Ideal for desktops and laptops

5) Use anacron when a job has to be executed irrespective of hour and

minute

**30)  Default Port numbers used by ssh,ftp,http,https,telnet,smtp,pop3,pop3s,imap,imaps**

SSH 22, ftp 20/21, http 80, https 443, SMTP/SMPTS 25/465, POP3/POP3S 110/995, IMAP/IMAPS 143/993

**31)  How to setup ACLs in following case:**

1) Create a file FILE1 and this should be read,write,executable for all user but Read only  for user USER1

2) Copy FILE1 ACLs to FILE2 ACL

3) Delete a USER1’s rule for FILE1 which were setup in step 1)

Ans 1) touch FILE1 ; chmod 777 FILE1 ; setfacl -m u:USER1:r FILE1

2) getfacl FILE1 | setfacl –set-file=- FILE2

3) setfacl -x u:USER1 FILE1

**32)  How to make USB bootable?**

Write efidisk.img from RHEL 6 DVD images/ subdirectory to USB

dd if=efidisk.img of=/dev/usb (usb device name)

**33)  How can we check disk/device status/failure/errors using smartctl utility?**

Try following to check:

Enable/Disable SMART on device/disk : smartctl -s on /dev/sda

Check device SMART health : smartctl -H /dev/sda

Check device SMART capabilities : smartctl -c /dev/sda

Enable/Disable automatic offline testing on device : smartctl -o on/off /dev/sda

Show device SMART vendor-specific Attributes and values : smartctl -A /dev/sda

Show device log [TYPE : error, selftest, selective, directory,background,

scttemp[sts,hist]] : smartctl -l TYPE /dev/sda

Run test on device [TEST: offline short long conveyance select,M-N pending,N

afterselect,[on|off] scttempint,N[,p] : smartctl -t /dev/sda

**34)  What is the difference between ext2 vs ext3 vs ext4?**

http://www.thegeekstuff.com/2011/05/ext2-ext3-ext4/

**35)  Disable ping to avoid network/ICMP flood**

Set following in /etc/sysctl.conf : net.ipv4.icmp\_echo\_ignore\_all = 1

Then “sysctl -p”

or

echo “1” > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all

**36)  What is SYN Flood, ICMP Flood**

SYN Flood : A **SYN flood** occurs when a host sends a flood of TCP/SYN packets, often with a

fake/forged sender address. Each of these packets is handled like a connection request, causing the

server to **spawn a half-open connection**, by sending back a **TCP/SYN-ACK packet**(Acknowledge), and

waiting for a packet in response from the sender address(response to the ACK Packet). However,

because the sender address is forged, the response never comes. These half-open connections

saturate the number of available connections the server is able to make, keeping it from responding to

legitimate requests until after the attack ends

ICMP Flood : There are three types of ICMP Flood :

1) Smurf Attack : http://en.wikipedia.org/wiki/Smurf\_attack

2) Ping Flood :  http://en.wikipedia.org/wiki/Ping\_flood

3) Ping of Death : http://en.wikipedia.org/wiki/Ping\_of\_death

**37)  What is the difference between Unix vs Linux Kernels?**

Please find below given link :

http://www.thegeekstuff.com/2012/01/linux-unix-kernel/

**38) How to setup Password less remote login/ssh?**

Use “**ssh-keygen -t dsa or rsa**” at local system for creating public and private keys

Then copy /root/.ssh/id\_dsa.pub to remote\_server by name /root/.ssh/authorized\_keys

Change permissions of /root/.ssh/authorized\_keys file at remote\_server “chmod 0600 ~/.ssh/authorized\_keys”

Now try to login from local system to remote\_server “ssh root@remote\_server”

**39) Command to see default kernel image file**

“grubby –default-kernel”

**40) How to create lvm mirror**

lvcreate -L 50G -m1 -n LVMmirror vg0

**41) Command to check last runlevel**

who -r

**42) What do you mean by File System?**

File System is a method to store and organize files and directories on disk. A file system can have different formats called file system types. These formats determine how the information is stored as files and directories.

**43) What is the requirement of udev daemon?**

Create and remove device nodes or files in /dev/ directory

**44) What are block and character devices?**

Both the devices are present in /dev directory

Block device files talks to devices block by block [1 block at a time (1 block = 512 bytes to 32KB)].

Examples: – USB disk, CDROM, Hard Disk (sda, sdb, sdc etc….)

Character device files talk to devices character by character.

Examples: – Virtual terminals, terminals, serial modems, random numbers (tty{0,1,2,3……})

**45) How to Convert ext2 to ext3 File System?**

**tune2fs -j /dev**/{device-name}

**46) File required to modify for setting up kernel parameters permanent**

**/etc/sysctl.conf**

**47) Commands used to install, list and remove modules from kernel**

Installing/adding a module:

insmod mod\_name

modprobe mod\_name

List installed modules :  lsmod

Removing a module     : modprobe -r mod\_name

**48) How to create swap using a file and delete swap**

Adding swap :

**dd if=/dev/zero of=/opt/myswap bs=1024 count=4**

**mkswap /opt/myswap**

swapon -a

For adding this myswap at boot time, add following in **/etc/fstab file**:

**/opt/myswap       swap     swap   defaults   0 0**

Deleting Swap :

Run “swapoff /opt/myswap” command

Remove the entry from /etc/fstab file

Remove /opt/myswap file (using rm command)

**49) What vmstat show**

vmstat (virtual memory statistics) is a computer system monitoring tool that collects and displays summary information about operating system memory, processes, interrupts, paging and block I/O

**50) What is tmpfs File System**

Reference : http://en.wikipedia.org/wiki/Tmpfs

tmpfs is a common name for a temporary file storage facility on many Unix-like operating systems. It is intended to appear as a mounted file system, but stored in volatile memory instead of a persistent storage device. A similar construction is a RAM disk, which appears as a virtual disk drive and hosts a disk file system.

Everything stored in tmpfs is temporary in the sense that no files will be created on the hard drive; however, swap space is used as backing store in case of low memory situations. On reboot, everything in tmpfs will be lost.

The memory used by tmpfs grows and shrinks to accommodate the files it contains and can be swapped out to swap space.

**51) What is the difference between screen and script commands?**

Screen is an screen manager with VT100/ANSI terminal emulation and used to take GNU screen session remotely or locally and while Script make typescript of terminal session

Screen : needs to be detached, should not be exited to access remotely/locally

Script : creates a file and store all the terminal output to this file

**52) How can we check which process is assigned to which processor?**

Ans Run “ps -elFL” and find out the PSR column which is showing the processor number to the process

**53) How can we check vendor, version, release date, size, package information etc… of any installed rpm?**

rpm -qi package-name , for example:

rpm -qi ypbind-1.19-12.el5