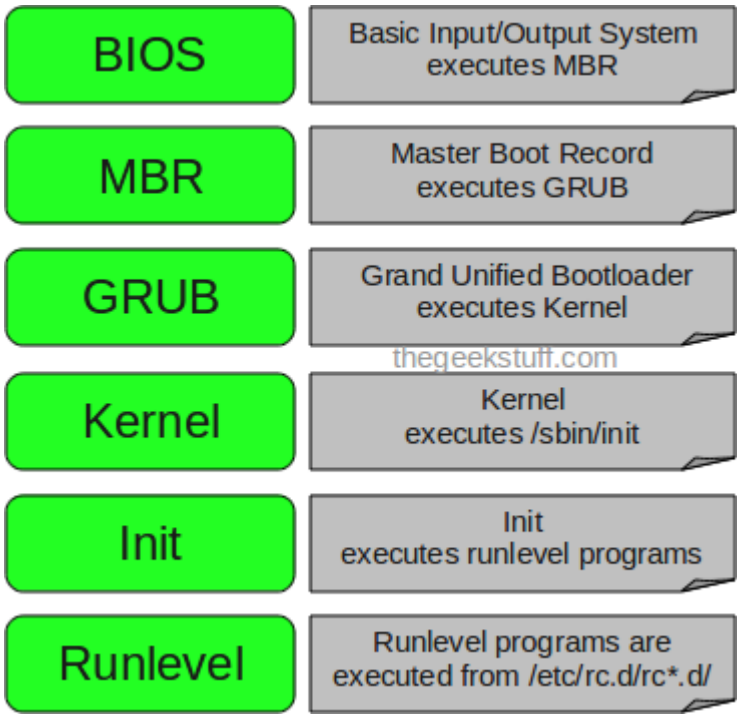
6 Stages of Linux Boot Process (Startup Sequence)

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



1. 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 is detected and loaded into the memory, BIOS gives the control to it.
- So, in simple terms BIOS loads and executes the MBR boot loader.

2. 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.

3. GRUB

- GRUB stands for Grand Unified Bootloader.
- If you have multiple kernel images installed on your system, you can choose which one to be executed.
- GRUB displays a splash screen, waits for few seconds, if you don't 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 didn't 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.

```
#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
```

- 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.

4. 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 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.

5. Init

- Looks at the /etc/inittab file to decide the Linux run level.
- 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.

6. 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

What is the SMTP ?

- SMTP is the most common protocol for an e-mail server.

What is NNTP ?

- NNTP is the common protocol which is used for news services. LeafNode and INN are examples of news servers.

You company wants to run Web Server on their intranet. Which Linux package should you use for this ?

To run a Web server, you should install the Apache Web server.

You company have slow internet connection. Which Linux service you can use to manage internet connection ?

You should use Squid proxy server, which allows to manage the web contents and also cache the web pages to decrease the amount of traffic going to Internet.

You have tasked with implementing new Linux systems in your lab, those will be used in training of Linux. What type of Linux distribution should you choose?

For LAB environment you can use free Linux version of Linux distribution. In test system at company or in a Lab environment where usually no real risk in making mistakes you should use free version of Linux. While distribution itself maybe free or nearly free, you will be required to pay for technical support. In Lab environment where time permits you, instead of seeking helping hands, try to solve the issue at your own, that could a great learning experience.

You have tasked with implementing a new Linux server in your network that will store confidential information of company. Your lab technician have fedora. Should you use it for your new server?

You could use it, but you should not use it for server. It is not recommended to use an obscure, unsupported distribution for critical server. A well-know, well-supported distribution like RHEL would be a better choice. If a technical problem occurs at some point after the server has been installed, you need to be able to call someone and get an answer immediately rather than searching on internet to find a solution. You should be able to solve the issue and get the server back into production as fast as possible.

You are installing a Linux system that will run a software that creates very large log files. Which directory should you create separate partition for ?

Create a separate partition at /var directory.

You are installing a Linux system that will provide file storage for a number of network users. Which directory should you create separate partition for?

Create a separate /home directory.

Which port should you open in your host firewall to run web server?

By default web server use port 80 and 443 which you need to open in firewall.

Which IP addressing should you use for Server?

For server you should always use static IP address.

Which IP address should you use for client desktop?

For client you can use both static and dynamic method. For easy management using DHCP to assign IP address would be the best option.

You are installing RHEL in new system that will be used by software developer to develop advance program. Which option should you choose during the installation, while installation program ask you to choose the set of software?

Choose Software Development Workstation and use customize now option to select additional packages.

You are installing RHEL in new system that will used by an administrative assistant to type documents, create presentations, and manage e-mail. Which option should you choose during the installation, while installation program ask you to choose the set of software?

Choose Desktop and use customize now option to select additional packages.

Which partition is used for virtual memory by a Linux system?

swap

Which ports should you open in host firewall for an email server?

- Open port 110 which is used by the POP3 e-mail protocol.
- Open port 25 which is used by the SMTP e-mail protocol.
- Open port 143 which is used by the IMAP e-mail protocol.

Your Linux system have two SCSI hard disk drives. The first drive is assigned as SCSI ID 0, and the second drive is assigned SCSI ID 1. How these will be refers in system?

/dev/sda point to the first SCSI drive.

/dev/sdb points to the second SCSI drive

Your Linux system have a single IDE hard disk drive. How partitions will be refers on the IDE drive?

- **hd** refers for IDE hard disk
- **a** refers for first hard disk. If system have multiple hard disk use b for second, c for third and so on till last hard disk.
- **1** refers for first partition, 2 for second partition and so on till last partition.

For example

- /dev/hda1 points to the first partition on the first IDE
- /dev/hdd4 points to the fourth partition on the fourth IDE
- /dev/hdc2 points to the second partition on the third IDE

Which file have runlevel configuration?

/ect/inittab

What command would you use to shut down the system in 100 seconds?

#shutdown -h 100

What daemon controls the print spooling process?

The Line Printing Daemon (lpd) controls the print spooling process.

What configuration file defines the default runlevel for the init process?

/etc/inittab file defines the default runlevel for the init process.

A user wants to restart the NFS server because they want to enable changes made in the configuration file. What command accomplishes this task?

#service nfs reload

The reload command will tell the system to stop the service, reload the configuration file, and restart the service

What command can you use to reboot a Linux system?

The command to reboot a Linux system is reboot

What mode must you be in when using vi editor to input text into a file?

To insert text in the vi editor, you must be in insert mode

Which utility could you use to repair the corrupted file system?

You can use fsck to repair the corrupted file system.

What must you do before performing fsck on a file system?

The fsck utility can only run on a file system that is unmounted. If it were active, fsck would not be able to properly repair the drive, and may cause further corruption.

A Linux administrator wants to review the messages that scrolled up the screen during a system boot. How can this be accomplished?

The boot kernel messages are saved to the log file /var/log/dmesg. He can check this file.

A user complains you that his system was running fine, before he rebooted. When it starts up, no display appears on the screen and the system is beeping. What may this indicate?

Because the system was running fine before reboot and during the it got problem even before the operating system is loaded, the problem is hardware-based, and is most likely caused by a problem with the system board.

A user has sent an e-mail, but within minutes the e-mail is returned stating that the address could not be found. What is the most likely cause of the error?

If the e-mail was returned, all mail services are working properly, but the destination e-mail address was wrong.

Your system crashed and being restarted, but a message appears, indicating that the operating system cannot be found. What is the most likely cause of the problem ?

This kind of problem most likely to be associated with hard disk. There might be some issue with either MBR or hard disk.

A user can not access a remote server. Which command he can use to verify that remote server is up?

He can use ping command to check whatever remote server is up or not.

A newbie administrator is having tough time to locate the httpd.conf file. What command line tool he can use to find file?

He should first try with locate command. find command would be his next tool.

A user has decided to come into work overnight to get some work done. Unfortunately, he is not able to login, even though he is using his proper name and password. What is the most likely cause of the problem?

In high security environments some organizations choose to implement time restrictions on accounts, so user would not be able to login after office time.

A Linux administrator is noticing odd system behavior. Which log file should he check to find general system log messages?

The general log stored in /var/log/messages file.

Instead of properly shutting down a Linux system, an user mistakenly just turned the machine off with the on/off switch. What will happen when the system restarts?

When the system shuts down abnormally and the file systems are not properly mounted, the fsck utility will automatically check the disks for errors and inconsistencies in order to repair them.

A newbie system admin is having trouble with the options for a particular command. What is the best resource to use for information on the command?

He can use man command to get detail of the options. A quick way to get help about options is to use --help option. Most Linux command support this option and return with brief information on how to use that command.

You are tasked to examine a log file in order to find out why a particular application keep crashing. Log file is very lengthy, which command can you use to simplify the log search using a search string ?

You can use grep command to output the log file. You can specify the keyword of desired application to look for, grep command than displays all instances of that word in log file.

A user is trying to check his mail by using the pop3 protocol and port 143. But mail program could not connect to the mail server to retrieve mail. What is the most likely cause of the problem?

User is using wrong port number. Port number 143 is used for imap, he should use port 110 instead of 143.

A developer is constantly making changes in his applications source file, then running application to see if is throwing any error. Which command can he use to see the log file in real time, instead of reopening the log file each time?

He can use tail command with -f options to see a file being updated in real time. He do not need to reopen the file to see any changes.

An administrator has made changes to a daemon's configuration file. When he checks the process, it is still running with old behavior. What is the reason behind it?

He need to restart the service to process can read and implement the new configuration.

An application process has just failed on a Linux system. What should you examine first to find out the root of the problem?

When an application fails, the first thing that you should do to help troubleshoot the problem is to examine the application logs for the particular error that caused the application to fail.

During a software package installation, an error occurs warning that a certain library is missing, and the installation aborts. What is the most likely cause of the problem?

Many software packages are dependent on other programs to function properly. If these dependencies do not exist, you must install them before installing your software package.

What command should be used to show the first 10 lines of a file?

The command to show the first 10 lines of a file is head -100 filename.

What command can an administrator use to see the status of a print queue?

The lpq command can be used to see the status of a print queue.

What is an INODE?

All files have its description stored in a structure called 'inode'. The inode contains info about the file-size, access and modification time, permission and so on. In addition to descriptions about the file, the inode contains pointers to the data blocks of the file.

State the syntax of any Linux command.

The correct syntax of Linux command is Command [options] [arguments]. **Master the Linux command line with this guide**.

What is the difference between TCP and UDP?

The basic difference is that TCP establishes a connection before sending data and this allows it to control the dataflow and guarantee that all packets get delivered. UDP simply chucks datagrams onto the wire and if some get lost or arrive in bad order there's no way to request a resend. However UDP has low network overhead so some services such as DNS resolution, SNMP, DHCP, RIP and VOIP use UDP for its speed and any errors are usually dealt with on the application layer rather than network layer.

How does DNS resolution work?

A client application requests an IP address from the name server usually by connecting to UDP port 53. The name server will attempt to resolve the FQDN based on its resolver library, which may contain authoritative information about the host requested or cached data about that name from an earlier query. If the name server does not already have the answer, it will turn to root name servers to determine the authoritative for the FQDN in question. Then, with that information, it will query the authoritative name servers for that name to determine the IP address.

What is an MX record?

An MX record numerically ranks the mail servers you would prefer to receive email for a domain. The MX record with the lowest number is preferred over the others, but you can set multiple email servers with the same value for simple load balancing.

Please describe the Linux boot-up sequence.

There are seven steps to the boot-up sequence. 1) BIOS (basic input/output system) – executes the MBR where Boot Loader sits, 2) MBR- Master boot reads Kernel into memory, 3) GRUB (Grand Unified Bootloader) Kernel starts Init process, 4) Kernel – Kernel executes the /sbin/init program. Init reads inittab, executes rc.sysinit, 5) Init – the rc script than starts services to reach the default run level and 6) Run level programs – these programs are executed from /etc/rc.d/rc*.dl/

How do you search for a pattern and then replace it in an entire file?

You use Sed, or in Vi editor, the search uses character ‘s’ slash the pattern to be searched, slash the pattern to replace it with, slash ‘g’ which stands for entire file.

How do you list and flush all IPtables?

First you use the –L switch to view all the currently present rules and then –F to flush them.

What is a shell? What are their names?

The shell is the part of the system with which the user interacts. A Unix shell interprets commands such as “pwd”, “cd” or “traceroute” and sends the proper instructions to the actual operating system itself. The shells currently available areAns SH, BASH, CSH, TCSH, NOLOGIN, KSH. Other functions of a shell include scripting capability, path memory, multitasking, and file handling.

What is a zombie?

Cheeky answers get bonus points for this one. But in the Linux world, a zombie process is the process output of 'ps' by the presence of 'Z' in the STAT column. Zombies are essentially the premature processes whose mature parent processes died without reaping its children. Note that zombies can't be killed with the usual 'kill' signal.

We hope this questions have helped you in your Linux interview preparation. If you'd like a more advanced tutorial on Linux and running Linux administration, learn to run **Linux servers from scratch here**.

Name the Linux services which provides network printing.

CUPS provide network printing between Linux systems. It can be used with Samba service to extend network printing to windows systems.

Which Linux service is used to provide network file storage ?
NFS service is used to provide file sharing.

Which Linux service is used as a database server ?
MySQL and PostgreSQL are Linux database server.

Which Linux service is used to turn a Linux system in proxy server ?
Squid service can be used to turn any Linux system into an in proxy server.

Which standard directory is used by vsFTP server for file sharing ?
Default Standard directory for ftp is /var/ftp/pub.

Which standard directory is used by Apache web server for HTML files ?
standard directory for HTML files is /var/www/html

What is the default partition layout during the installation ?
Default partition Layout is the LVM.

Which necessary partition cannot be a part of logical volume group ?
boot partition cannot be a part of logical volume group. You must have create it as a regular partition.

Which partitions are recommended for custom layout of partition ?

- /

- /boot
- /home
- Swap
-

What step during the installation could you take to prevent a program from creating temporary files that fill up the entire space ?

You can create a separate /tmp partition prevents a program from creating temporary files that fill up the entire filesystem.

What is the kickstart ?

kickstart is a installation method used in RHEL. A kickstart installation is started from a kickstart file, which contains the answers to all the questions in the installation program.

Name any of two third party distribution based on RHEL6 source code.

CentOS and Scientific Linux

Which Log file contains all installation message?

install.log.syslog file contains all messages that were generated during the installation.

Why LVM is required ?

LVM stands for Logical Volume Manager , to resize filesystem's size online we required LVM partition in Linux. Size of LVM partition can be extended and reduced using the lvextend & lvreduce commands respectively.

How To check Memory stats and CPU stats ?

Using 'free' & 'vmstat' command we can display the physical and virtual memory statistics respectively.With the help of 'sar' command we see the CPU utilization & other stats.

What does Sar provides and at which location Sar logs are stored ?

Sar Collect, report, or save system activity information. The default version of the sar command (CPU utilization report) might be one of the first facilities the user runs to begin system activity investigation, because it monitors major system resources. If CPU utilization is near 100 percent (user + nice + system), the workload sampled is CPU-bound.
By default log files of Sar command is located at /var/log/sa/sadd file, where the dd parameter indicates the current day.

How to increase the size of LVM partition ?

Below are the Logical Steps :
– Use the lvextend command (lvextend -L +100M /dev/<Name of the LVM Partition> , in this example we are extending the size by 100MB.
– resize2fs /dev/<Name of the LVM Partition>
– check the size of partition using 'df -h' command

Q:5 How to reduce or shrink the size of LVM partition ?

Ans: Below are the logical Steps to reduce size of LVM partition :
-Umount the filesystem using umount command,
-use resize2fs command , e.g resiz2fs /dev/mapper/myvg-mylv 10G
-Now use the lvreduce command , e.g lvreduce -L 10G /dev/mapper/myvg-mylv
Above Command will shrink the size & will make the filesystem size 10GB.

Q:6 How to create partition from the raw disk ?

Ans: Using fdisk utility we can create partitions from the raw disk.Below are the steps to create partition from the raw dsik :
– fdisk /dev/hd* (IDE) or /dev/sd* (SCSI)
– Type n to create a new partition
– After creating partition , type w command to write the changes to the partition table.

Where the kernel modules are located ?

The '/lib/modules/kernel-version/' directory stores all kernel modules or compiled drivers in Linux operating system. Also with 'lsmod' command we can see all the installed kernel modules.

What is umask ?

umask stands for 'User file creation mask', which determines the settings of a mask that controls which file permissions are set for files and directories when they are created.

How to set the umask permanently for a user?

To set this value permanently for a user, it has to be put in the appropriate profile file which depends on the default shell of the user.

How to change the default run level in linux ?

To change the run level we have to edit the file "/etc/inittab" and change initdefault entry (id:5:initdefault:). Using 'init' command we change the run level temporary like 'init 3' , this command will move the system in runlevl 3.

How to share a directory using nfs ?

To share a directory using nfs , first edit the configuration file '/etc/exportfs' , add a entry like '/<directory-name> <ip or Network>(Options)' and then restart the nfs service.

How to check and mount nfs share ?

Using 'showmount' command we can see what directories are shared via nfs e.g 'showmount -e <ip address of nfs server>'.Using mount command we can mount the nfs share on linux machine.

What are the default ports used for SMTP,DNS,FTP,DHCP,SSH and squid ?

Service	Port
SMTP	25
DNS	53
FTP	20 (data transfer) , 21 (Connection established)
DHCP	67/UDP(dhcp server) , 68/UDP(dhcp client)
SSH	22
Squid	3128
TELNET	23
HTTP	80
POP3	110
NTP	123
SMB	139
IMAP	143
LDAP	389
HTTPS	443
MYSQL	3306
NFS	2049

What is Network Bonding ?

Network bonding is the aggregation of multiple Lan cards into a single bonded interface to provide fault tolerance and high performance. Network bonding is also known as NIC Teaming.

What are the different modes of Network bonding in Linux ?

Below are list of modes used in Network Bonding :
balance-rr or 0 – round-robin mode for fault tolerance and load balancing.
active-backup or 1 – Sets active-backup mode for fault tolerance.
balance-xor or 2 – Sets an XOR (exclusive-or) mode for fault tolerance and load balancing.
broadcast or 3 – Sets a broadcast mode for fault tolerance. All transmissions are sent on all slave interfaces.
802.3ad or 4 – Sets an IEEE 802.3ad dynamic link aggregation mode. Creates aggregation groups that share the same speed & duplex settings.
balance-tlb or 5 – Sets a Transmit Load Balancing (TLB) mode for fault tolerance & load balancing.
balance-alb or 6 – Sets an Active Load Balancing (ALB) mode for fault tolerance & load balancing.

How to check and verify the status the bond interface.

Using the command ‘cat /proc/net/bonding/bond0’ , we can check which mode is enabled and what lan cards are used in this bond. In this example we have one only one bond interface but we can have multiple bond interface like bond1,bond2 and so on.

How to check default route and routing table ?

Using the Commands ‘netstat -nr’ and ‘route -n’ we can see the default route and routing tables.

How to check which ports are listening in my Linux Server ?

Use the Command ‘netstat –listen’ and ‘lsof -i’

List the services that are enabled at a particular run level in linux server ?

With the help of command ‘chkconfig –list | grep 5:on’ we can list all the service that are enabled in run level5. For other run levels just replace 5 with the respective run level.

How to enable a service at a particular run level ?

We can enable a service using the Command ‘chkconfig <Service-Name> on –level 3’

How to upgrade Kernel in Linux ?

We should never upgrade Linux Kernel , always install the new New kernel using rpm command because upgrading a kenel can make your linux box in a unbootable state.

How To scan newly asssigned luns on linux box without rebooting ?

There are two ways to scan newly assigned luns :
Method:1 if sg3 rpm is installed , then run the command ‘rescan-scsi-bus.sh’
Method:2 Run the Command , echo ” – – – ” > /sys/class/scsi_host/hostX/scan

How to find WWN numbers of HBA cards in Linux Server ?

We can find the WWN numbers of HBA cards using the command ‘systool -c fc_host -v | grep port_name’

How to add & change the Kernel parameters ?

To Set the kernel parameters in linux , first edit the file ‘/etc/sysctl.conf’ after making the changes save the file and run the command ‘sysctl -p’ , this command will make the changes permanently without rebooting the machine.

What is Puppet Server ?

Puppet is an open-source & enterprise software for configuration management toll in UNIX like operating system. Puppet is a IT automation software used to push configuration to its clients (puppet agents) using code. Puppet code can do a variety of tasks from installing new software, to check file permissions, or updating user accounts & lots of other tasks.

What are manifests in Puppet ?

Manifests in Puppet are the files in which the client configuration is specified.

Which Command is used to sign requested certificates in Puppet Server ?

'puppetca –sign hostname-of-agent' in (2.X) & 'puppet ca sign hostname-of-agent' in (3.X)

At which location Puppet Master Stores Certificates ?

/var/lib/puppet/ssl/ca/signed

How to find all the regular files in a directory ?

using the command 'find /<directory -type f'.

What is load average in a linux ?

Load Average is defined as the average sum of the number of process waiting in the run queue and number of process currently executing over the period of 1,5 and 15 minutes. Using the 'top' and 'uptime' command we find the load average of a linux sever.

What is cpio command ?

cpio stands for Copy in and copy out. Cpio copies files, lists and extract files to and from a archive (or a single file).

How to check the SPF record of domain from command line ?

We can check SPF record of a domain using dig command. Example is shown below :
linuxtechi@localhost:~$ dig -t TXT google.com

How to identify which package the specified file (/etc/fstab) is associated with in linux ?

rpm -qf /etc/fstab
Above command will list the package which provides file "/etc/fstab"

Which command is used to check the status of bond0 ?

cat /proc/net/bonding/bond0

What is the use of /proc file system in linux ?

The /proc file system is a RAM based file system which maintains information about the current state of the running kernel including details on CPU, memory, partitioning, interrupts, I/O addresses, DMA channels, and running processes. This file system is represented by various files which do not actually store the information, they point to the information in the memory.
The /proc file system is maintained automatically by the system.

How to find files larger than 10MB in size in /usr directory ?

find /usr -size +10M

How to find files in the /home directory that were modified more than 120 days ago ?

find /home -mtime +l20

How to find files in the /var directory that have not been accessed in the last 90 days ?

find /var -atime -90

Search for core files in the entire directory tree and delete them as found without prompting forconfirmation

find / -name core -exec rm {} \;

What is the purpose of strings command ?

The strings command is used to extract and display the legible contents of a non-text file.

What is the use tee filter ?

The tee filter is used to send an output to more than one destination. It can send one copy of the output to a file and another to the screen (or some other program) if used with pipe.
linuxtechi@localhost:~$ ll /etc | nl | tee /tmp/ll.out
In the above example, the output from ll is numbered and captured in /tmp/ll.out file. The output is also displayed on the screen.

What would the command export PS1 = ”$LOGNAME@`hostname`:\$PWD: do ?

The export command provided will change the login prompt to display username, hostname, and the current working directory.

What would the command ll | awk '{print $3,"owns",$9}' do ?

The ll command provided will display file names and their owners.

What is the use of at command in linux ?

The at command is used to schedule a one-time execution of a program in the future. All submitted jobs are spooled in the /var/spool/at directory and executed by the atd daemon when the scheduled time arrives.

What is the role of lspci command in linux ?

The lspci command displays information about PCI buses and the devices attached to your system. Specify -v, -vv, or -vvv for detailed output. With the -m option, the command produces more legible output.

What is the difference between umask and ulimit ?

umask stands for 'User file creation mask', which determines the settings of a mask that controls which file permissions are set for files and directories when they are created. While ulimit is a linux built in command which provides control over the resources available to the shell and/or to processes started by it.

You can limit user to specific range by editing /etc/security/limits.conf at the same time system wide settings can be updated in /etc/sysctl.conf

What are the run levels in linux and how to change them ?

A run level is a state of init and the whole system that defines what system services are operating and they are identified by numbers.There are 7 different run levels present (run level 0-6) in Linux system for different purpose. The descriptions are given below.

0: Halt System (To shutdown the system)
1: Single user mode
2: Basic multi user mode without NFS
3: Full multi user mode (text based)
4: unused
5: Multi user mode with Graphical User Interface
6: Reboot System

To change the run level, edit the file "/etc/inittab" and change initdefault entry (id:5:initdefault:). If we want to change the run level on the fly, it can be done using 'init' command.

For example, when we type 'init 3' in the commandline , this will move the system from current runlevel to runlevl 3. Current level can be listed by typing the command 'who -r'

What is the functionality of a Puppet Server ?

Puppet is an open-source and enterprise application for configuration management toll in UNIX like operating system. Puppet is an IT automation software used to push configuration to its clients (puppet agents) using code. Puppet code can do a variety of tasks from installing new software, to check file permissions, or updating user accounts and lots of other tasks.

What is SeLinux?

SELinux is an acronym for Security-enhanced Linux. It is an access control implementation and security feature for the Linux kernel. It is designed to protect the server against misconfigurations and/or compromised daemons. It put limits and instructs server daemons or programs what files they can access and what actions they can take by defining a security policy.

What is crontab and explain the fields in a crontab ?

The cron is a deamon that executes commands at specific dates and times in linux. You can use this to schedule activities, either as one-time events or as recurring tasks. Crontab is the program used to install, deinstall or list the tables used to drive the cron daemon in a server. Each user can have their own crontab, and though these are files in /var/spool/cron/crontabs, they are not intended to be edited directly. Here are few of the command line options for crontab.

crontab -e Edit your crontab file.

crontab -l Show your crontab file.

crontab -r Remove your crontab file.

Traditional cron format consists of six fields separated by white spaces:

The format is explained in detail below.

```
* * * * * *
| | | | | |
| | | | | +– Year (range: 1900-3000)
| | | | +—- Day of the Week (range: 1-7, 1 standing for Monday)
| | | +—— Month of the Year (range: 1-12)
| | +——– Day of the Month (range: 1-31)
| +———- Hour (range: 0-23)
+———— Minute (range: 0-59)
```

What are inodes in Linux ? How to find the inode associated with a file ?

An inode is a data structure on a filesystem on Linux and other Unix-like operating systems that stores all the information about a file except its name and its actual data. When a file is created, it is assigned both a name and an inode number, which is an integer that is unique within the filesystem. Both the file names and their corresponding inode numbers are stored as entries in the directory that appears to the user to contain the files. The concept of inodes is particularly important to the recovery of damaged filesystems. When parts of the inode are lost, they appear in the lost+found directory within the partition in which they once existed.

The following will show the name of each object in the current directory together with its inode number:

```
# ls -i
```

The avialble number inodes in a filesystem can be found using the below command :

```
# df -i
```

The other way we can get the inode details of a file by using the stat commmand.

Usage : # stat

Example :

```
-sh-4.1$ stat note.txt
File: `note.txt'
Size: 4 Blocks: 8 IO Block: 4096 regular file
Device: fd05h/64773d Inode: 8655235 Links: 1
Access: (0644/-rw-r--r--) Uid: (69548/nixuser) Gid: (25000/ UNKNOWN)
Access: 2014-06-29 15:27:56.299214865 +0000
Modify: 2014-06-29 15:28:28.027093254 +0000
Change: 2014-06-29 15:28:28.027093254 +0000
```

Apart from the above basic questions, be prepared for answers for the below questions

1. How to set linux file/directory permissions ?

2. How to set ownership for files/directories ?

3. How to create user/group and how to modify it ?

4. How to find kernel / OS version and its supported bit (32/64) version ?

5. How to set / find interface ip address ?

6. How to find linux mount points and disk usage ?

7. What command to find memory and swap usage ?

8. Have a look on ps, top, grep, find, awk and dmesg commands ?

Explain Booting procedure or steps in Linux?

1.Once System powered on, it automatically invokes BIOS
2. BIOS will start the processor and perform a POST [power on self test] to check the connected device are ready to use and are working properly.
3. After POST , BIOS will check for the booting device. The boot sector is always the first sector of the hard disk and BIOS will load the MBR into the memory.
MBR holds the boot loader of the OS.
4. Then boot loader takes the control of the booting process.
5. GRUB is the boot loader for Linux.
6. Depending on the boot option selected the kernel is loaded first.
7. After kernel is loaded the kernel will take the control of the booting process
8. Initrd will be loaded which contains drivers to detect hardware (its called Initialization of RAM Disk)
9. Then it will initialize all the hardware including I/O processors etc.
10. Kernel will mounts the root partition as read-only
11. INIT is loaded as the first process.
12. INIT will mount the root partition and other partitions as read/write and checks for file system errors.
13. Sets the System Clock, hostname etc..
14. Based on the Runlevel, it will load the services and runs the startup scripts which are located in /etc/rcX.d/ (Network, nfs, SSH etc.)
15. Finally it runs the rc.local script & Now the login prompt will appear.

What is stage 1.5 boot loaded in linux?

The great thing about GRUB is that it includes knowledge of Linux file systems. Instead of using raw sectors on the disk, as LILO does,
GRUB can load a Linux kernel from an ext2 or ext3 file system. It does this by making the two-stage boot loader into a three-stage boot loader.

A. Stage 1.5 boot loader , it contains extra coe to allow cylinders above 1024, or LBA type drives, to be read.
B. It will be stored on MBR or Boot partition .
C. Stage 1 (MBR) boots a stage 1.5 boot loader that understands the particular file system containing the Linux kernel image.
D. Basically this module will load the knowledge of Filesystem to Grub to read the kernel
so ,
Stage 1 Boot loaded is : MBR
Stage 1.5 Boo loader : e2fs_stage1_5
Stage 2 Boot loader is : GRUB

How to reinstall GRUB?

A.Boot up using RHEL4 disk.
B.Enter into rescue mode
#linux rescue (hit ok)
C. Then follow below commands
# chroot /mnt/sysimage
# grub
# find /boot/grub/stage1 or find /grub/stage1
root(hd0,0) //example o/p
Now install the GRUB
setup (hd0)
EXIT
Another Method
#linux rescue
chroot /mnt/sysimage
/sbin/grub-install /dev/hda

Linux Booting Issues : How to solve ??

Option 1: init not found error
Option 2: Run fsck on all FS in rescue mode
Option 3: Reinstall GRUB
Option 4: Recover grub.conf / grub configuration

Option 1: For normal panic and "init not found" error.

Error : "init not found" displayed

1) Launch the system to Bash shell prompt

Reboot the server and interrupt to edit the GRUB.

Edit grub and enter the below in last

init=/bin/bash

Then save and exit and boot the server. This will launch you straight into a Bash shell prompt.Then you can remount "/" file system and check /var/log/messages for any error.

Note : init=/bin/bash (Grub boot loader) or linux init=/bin/bash (if Lilo boot loader).

2) Once server booted and if it is in Bash shell prompt

#mount -o remount,rw /

3) Now you can check the log messages and try to find the reason for server pacnic or error.

#more /var/log/messages

Option 2: If the above option not helped then follow the next

1) Boot from the Linux First CD (boot CD).

2) Type "boot rescue" at Linux boot prompt.

3) After the bash shell prompt show up, type the below command

chroot /mnt/sysimage

a) Run fsck and Check for any disk error

#fdisk -l /dev/sda //check how many partion you have

then run fsck on each partition

#fsck -y /dev/sda2'

Option 3: If the above also not helped then reinstall grub and retry.

In rescue mode.

chroot /mnt/sysimage

/sbin/grub-install /dev/had

Option 4: If a system has issues with the GRUB configuration

(possibly caused by incorrect changes to the the GRUB configuration file, installation of another OS, changes to device ordering due to hardware or BIOS changes, etc.)

grub> find /boot/grub/grub.conf (or) grub>find /grub/grub.conf (or) find /boot/grub/stage1

(hd0,1)

(hd1,2)

>> This tells us that we have two /boot partitions. Then we have to reinstall the GRUB config on disk (one by one) and try.

#grub> root (hd0,1) //Write the GRUB bootloader on the MBR of the first disk

grub> setup (hd0)

grub>quit

If you have doubt as to where the root partition is located then try to find a file in /etc.

#grub> find /etc/fstab

(hd0,1)

Note: You must pay attention to your devices, for me "hd0" is the root disk and (hd0,1) is /boot partition , and (hd0,1) is my ROOT (/) partition. mostly / "root" partion will be on LVM.

You might not even have "hd0" mapped out. Review your "/boot/grub/device.map" file

#cat /boot/grub/device.map

How to recover or rest Root password in LINUX?

While booting

1. Select the kernel
2. Press the "e" key to edit the entry
3. Select second line (the line starting with the word kernel)
4. Press the "e" key to edit kernel entry so that you can append single user mode
5. Append the letter "S" (or word Single) to the end of the (kernel) line
6. Press ENTER key
7. Now press the b key to boot the Linux kernel into single user mode
8. At prompt type passwd command to reset password:

You need to mount at least / and other partitions:

mount -t proc proc /proc

mount -o remount,rw /

Change the root password,

passwd

thenreboot system:

sync

reboot

What is super Block and how will u recover it ?

The blocks used for two different purpose:

1.Most blocks stores user data aka files (user data).

2. Some blocks in every file system store the file system's metadata.

So what the hell is a metadata?

File system type
Size
Status
Information about other metadata structures

To find super block

#dumpe2fs /dev/sda3|grep -i superblock

or

mke2fs -n /dev/sda3

To repair file system by alternative-superblock use command as follows:

e2fsck -f -b 8193 /dev/sda3

What is the difference between service and process?

A process is any piece of software that is running on a computer. For example, your anti-virus software runs in the background as a process, which was automatically started when the computer booted. Some processes start when your computer boots, others are started manually when needed.Some processes are services that publish methods to access them, so other programs can call them as needed. Printing services would be an example of a service type of process, where your email program can just call the print services process to say it wants to print, and the service does the actual work.

How to view crond status? If it's show service is not found.

Service crond restart

My clients are getting services from servers but how to know which client is using which service. is there any files to keep information about these? Clients used ftp, nis, samba, apache, squid, nfs and mail services how to know how many users got service from server side with date, time and client system ip?

Mail server – /var/log/mail/maillog [RedHat,centos]
ssh – /var/log/secure
Apache – /var/log/http/access.log
nfs – /var/lib/nfs/rmtab

How to FTP user access other directory except his own home directory?

vim /etc/vsftpd/vsftpd.conf
Chroot_list_enable=yes

What are the Linux-based security tools?

Selinux
Firewall
iptables
Tcp-wrappers

What are the basic elements of firewall?

A firewall should be able to filter packets (drop/pass them) based on certain rules specified by the user. The rules may be used to identify an incoming packet to the computer or outgoing packet from the computer, it can be based on target port number/ip add , traffic from a particular Network card etc…

The firewall rules can be in a tabular form (saved on the disk) from where the firewall software can read them and implement it. iptables firewall on Linux is a great example

What is a command to display top 10 users who are using huge space?

du -sh /home/* | sort -r | head -10

How do find all failed login attempts via ssh?

tail -f /var/log/secure | grep Failed

How do you configure Linux system as a router?

vim /etc/sysctl.conf

net.ipv4.ip_forward=1

system-config-network

eth0 192.168.1.120 eth0:1 172.24.0.1

255.255.255.0 255.255.0.0

172.24.0.1 192.168.1.120

What is the UID and GID of root user? Can a normal user can change the ownership of a file? What is the command to change ownership of a file?

The root UID/GID is 0 (zero). Which is why he can able to intervene in all normal users files even though he don't had permission. A normal user will don't have the permission to change ownership of file. The command to change ownership is < chown user.user file >

What is the diff b/w ext2 and ext3?

Ext3 is a tiny bit slower than ext2 is, but it holds tremendous advantages. There is really only one difference between ext2 and ext3, and that is that ext3 uses a journal to prevent filesystem corruption in the case of an unclean shutdown (ie. before the filesystem is synced to disk). That makes ext3 a bit slower than ext2 since all metadata changes are written to the journal, and then flushed to disk, but on the other hand you don't risk having the entire filesystem destroyed at power failure or if an unwitted person turns the computer off uncleanly. You don't have to check the filesystem after an unclean shutdown either. Ext3 has three levels of journalling. Metadata (ie. internal filesystem structures) are always journalled, so that the filesystem itself is never corrupted. How ordinary data is written to the file system is controllable, though. The default option is the "ordered" mode, which causes file contents to be written to the filesystem before metadata is even committed to the journal. The highest reliable mode is called the "journal" mode, which causes file data to be committed to the journal before it is flushed to its final place, like the metadata. The least reliable mode, but rumoured to be the fastest, is called the "writeback" mode, which makes no promises at all regarding the consistency of file data. Only metadata is output reliably in writeback mode. So as for anything else, it's mainly a matter of priority. If you don't want ultimate speed, go

with ext3. If you need the highest speed that is theoratically aquirable though, then go with ext2. For that to be effective you'll probably need a really advanced hard drive controller, though.

As the system administrator you need to review Bob's cronjobs. What command would you use?
crontab –lu Bob

What command is used to remove the password assigned to a group?
gpasswd –r groupname

What are the different RAID levels?
- RAID level 0
- RAID level 1
- RAID level 2
- RAID level 3
- RAID level 4
- RAID level 5
- RAID level 6
- RAID level 10
- RAID level 50

How do you create a swapfile?
dd if=/dev/zero of=/swapfile bs=1024 count=200M
mkswap /swapfile
swapon /swapfile

What does nslookup do?
Nslookup is a program used to find information about internet Domain Name server.
The two modes of nslookup are: Interactive and non-interactive.
Using 'interactive mode' user can query the name servers for the information pertaining to hosts and domains.Using 'non-interactive mode' the user can just print the name and requested information of a host.

What is the difference between UDP and TCP?

TCP is a Transmission Control Protocol.
UDP is a User Datagram Protocol.
There are four major differences between UDP and TCP:
1. TCP can establish a Connection and UDP cannot.
2. TCP provides a stream of unlimited length, UDP sends Small packets.
3.TCP gurantees that as long as you have a connection data sent will arrive at the destination, UDP provides not guarantee delivery.
4.UDP is faster for sending small amounts of data since no connection setup is required, the data can be sent in less time then it takes for TCP to establish a connection.

What command do you run to check file system consistency?

Need to run fsck [file system consistency check] command to check file system consistency and repair a Linux / UNIX file system.
fsck

What is the command to remove Lvm ,Pv and vg

1st remove the entry on /etc/fstab file & save – quit.
2nd remove LVM – lvremove lvname
3rd remove VG – vgremove vgname
4th remove PV – pvremove pvname

How to create SAMBA server in fedora 9 Linux?

yum install samba –y
yum install samba-swat –y
vi /etc/samba/smb.conf

comment = windows sharing
path = path/your/share/directory
valid users = surendra
writable = yes
browseable = yes

then type testparm for code testing.

smbpasswd -a username
smbpasswd -e username

service smb restart
chkconfig smb on

How to schedule cron backup to run on 4th Saturday of month?

* * * * 6 weekdaynum 4 && sh /backup/test.sh

What is an inode?

ext2 and ext3 file systems keep a list of the files they contain in a table called an inode table. The inode is referenced by its number. This is unique within a file system.The inode contains the metadata about files. Among the data stored in the inode is
File type
File permissions
Link count

User ID number of the file owner and the group ID number of the associated group
Last modification time
Location of the data on the hard disk
Other metadata about the file
ls -li – view inode number only
stat /etc/passwd – view inode details

How to see unallocated hard disk space on linux
df -h

How do u find remote machine operating system and version?
nmap -A –v 192.168.1.100

How do you port scanning with netstat command?
netstat –an

inux system monitoring Tools?

top – Process Activity Command
vmstat – System Activity, Hardware and System Information
w – Find out Who Is Logged on And What They Are Doing
Uptime – Tell How Long the System Has Been Running
ps – Displays the Processes
free – Memory Usage
iostat – Average CPU Load, Disk Activity
sar – Collect and Report System Activity
mpstat – Multiprocessor Usage
pmap – Process Memory Usage

Linux Network monitoring Tools?

netstat and ss – Network Statistics
iptraf – Real-time Network Statistics
tcpdump – Detailed Network Traffic Analysis
strace – System Calls

/Proc file system – Various Kernel Statistics
cat /proc/cpuinfo
cat /proc/meminfo
cat /proc/zoneinfo
cat /proc/mounts

Nagios – Server And Network Monitoring
Cacti – Web-based Monitoring Tool
Gnome System Monitor – Real-time Systems Reporting and Graphing

What is mean by system calls?

A system call is the mechanism used by an application program to request service from the operating system.On Unix-based and POSIX-based systems, popular system calls are open, read, write, close, wait, exec, fork, exit, and kill. Many of today's operating systems have hundreds of system calls. For example, Linux has 319 different system calls. FreeBSD has about the same (almost 330). Tools such as strace and truss report the system calls made by a running process.

How do u extract files from iso cd images in linux?

mount –o loop disk1.iso /mnt/iso