**Finger :** Complete Information about all the users who are logged in

**Cut :** It divides a string or output

Cut [-d: delimeter,-f:particual field,-c:particular character] file

**Paste** : to join two or more files horizontally by using delimiters

**Diff :** different lines between 2 files

**Cmp :** it compares 2 files character by character

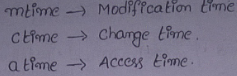
**Tr :** it translates character by character

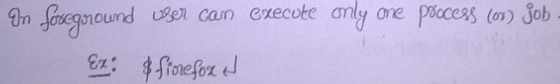
Aspellcheck : To check the spelling mistakes

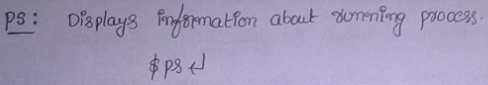
Pipe : combine 2 or more commands in a single line

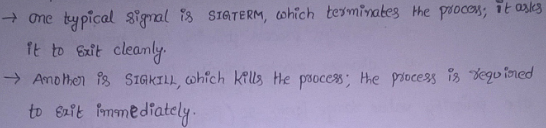
More/Less : To see the contents of a file by page wise

Find : this filter is used to search the results based on the requirements, size,type,permissions

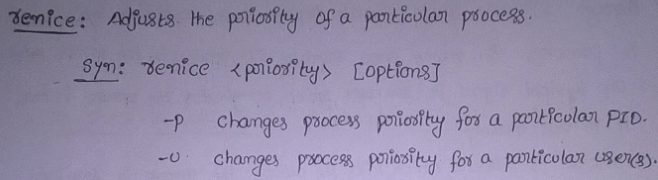












Partitioning means to divide a single hard drive into many logical drives

MBR --- IPL,PTI,Secondary bootloader

Primary partition

Extended –LVM

8e for Linux LVM, 82 for Linux Swap and 83 for Linux normal partition

# fdisk -l

# fdisk /dev/sdc

# partprobe /partx -a/kpartx /dev/sdc1

# mkfs.ext2/ext3/ext4/xfs/vfat

# mount /dev/sdc1 /mnt/oracle

# vim /etc/fstab

# e2label <device name or partition name><label name> (to assign the label to that partition)

# blkid <partition name or disk name> (to see the UUID or block id of that partition)

# mkswap <device or partition name> (to format the partition with swap file system)

# swapon -s (to see the swap usage)

**# fsck <device or partition name>**command we can check the integrity of the file system.

By using **# gparted**  command we can extend the root partition

It is a dedicated area in the file system where all the changes are tracked when the system crashed. So the possibility of the file system corruption or crashes is less because of this journaling feature.

# tune2fs -l /dev/sdb1 (to check whether the journaling is there or not)

# tune2fs -j /dev/sdb1 (to convert ext2 file system to ext3 file system)

# journalctl (It tracks all the log files between two different timings and by default saved in **/run/log** location)

# sar (sar utility is to watch the system activity report like CPU, memory,...etc.,)

Using this LVM we can extend or reduce the file systems as per requirement without loss of any data.

**# lvcreate -L +<size in MBs>**

# lvextend -L +<size in MB></dev/vgname/lvname> or

# lvresize -L +<size in MB></dev/vgname/lvname>

# resize2fs </dev/vgname/lvname>

# cat /etc/lvm/lvm.conf

RAID stands for Redundant Array of Independent Disks.

It provides fault tolerance, load balancing using stripping, mirroring and parity concepts

(i) RAID - 0 ---- Stripping ---- Minimum 2 disks required

(ii) RAID - 1 ---- Mirroring ---- Minimum 2 disks required

(iii) RAID - (1+0) --- Mirroring + Stripping ---- Minimum 4 disks required

(iv) RAID - (0+1) --- Stripping + Mirroring ---- Minimum 4 disks required

(v) RAID - 5 ---- Stripping with parity ---- Minimum 3 disks required

# mdadm

To search files and directories there are two commands.

(i) # locate

(ii) # find

locate always looks the locate database and not in a specific location. The data of the locate is stored in **/var/lib/mlocate/mlocate.db** file. **# updatedb** is the command to update the locate database. locate database cannot be find the newly created files and directories.

* User names and user id are stored in **/etc/passwd** file.
* User's passwords are stored in  **/etc/shadow** file in an encrypted form.
* And some user environmental files like .bash\_logout, .bash\_profile, .bashrc , ...etc., are also copied from **/etc/skell**  to his/her home directory (**/home/<username>**).
* **/etc/login.defs**  ----> user's login defaults settings information taken from this file.

**# pwunconv** (It creates the users according **/etc/passwd** file and deletes the **/etc/shadow** file) **.bash\_logout :** This is a user's logout ending program file. It will execute first whenever the user is logout.

**.bash\_profile :** This is user's login startup program file. It will execute first whenever the user is login. It consists the user's environmental variables.

**.bashrc :** This file is used to create the user's custom commands and to specify the umask values for that user's only.

The user file-creation mode mask (umask) is used to determine the file permissions for newly created files or directories

If we plan to allow all the users to execute the root users command then we go for set uid (suid).

If we plan to allow all the users of one group to get the group ownership permissions then we go for set gid

It protects the data from other users when all the users having full permissions on one directory.

**recover the root password if missed or deleted**

boot the system in single user mode.

(vi) Then prompt appears and type **# passwd root** command.

**How to restrict the users from login?**

(i) By removing (deleting) the user we can restrict the user from login.

(ii) Put the user's hostnames as entries in **/etc/hosts.deny** file (applying TCP wrappers).

(iii) **#passwd -l <user name>** (by locking his password we can restrict the users).

Define more access rights nothing but permissions to files and directories. Using Access Control list we assign the permissions to some particular users to access the files and directories.

# getfacl <options><file or directory name>

The options are, -d -----> Display the default ACLs.

# setfacl <options><argument> : <username>: <permissions><file or directory name>

The options are, -m -----> Modifies an ACL.

**How will you lock a user, if he enters wrong password 3 times?**

pam\_tally.so module maintains a count of attempted accesses, can reset count on success, can deny access if too many attempts fail. Edit /etc/pam.d/system-auth file, enter:  
 (i) # vi /etc/pam.d/system-auth

**account required pam\_tally.so deny=3 no\_magic\_root lock\_time=180**

**How to extend the logical volume to max. disk space and half of the disk space?**

# lvextend -l +100% FREE <logical volume> (to extend the logical volume by adding the volume group's total available space)

# lvextend -l 50% <vgname><lvname> (to extend the logical volume by adding the 50% free space of the volume group)

**How to put never expiry to a user?**

# passwd -x -1 <user login name>

**How to see the no. of failed logins of the users?**

# faillog -u <user name> (to see the specified users failed login attempts)

# faillog -a (to see failed login attempts of all users)

# faillog -M <Max. no> -u <user name> (to set Max. login failed attempts to that user)

# faillog -M 5 -u raju (to set Max. login failed attempts to 5 for user raju)

By configuring the disk quotas we can restrict the user to use unlimited space on the file system

# quotaon (to enable the quota)

# quotaoff (to disable the quota)

# edquota (to edit or modify the quota)

# repquota (to display or report the present quota)

# quotacheck (to create a quota database)

# chpasswd (to change multiple user's passwords)

<user name 1> : <password>

<user name 2> : <password>

. Protocols are generally use packet switching techniques to send and receive messages in the form of packets

|  |  |
| --- | --- |
| TCP/IP | UDP |
| Transmission Control Protocol | User Datagram Protocol |
| It is connection oriented | It is connection less |
| Reliable | Non-Reliable |
| TCP Acknowledgement will be sent / received | No Acknowledgement |
| Slow communication | Fast communication |
| Protocol No. for TCP is 6 | Protocol No. for UDP is 17 |
| HTTP, FTP, SMTP, ....etc., uses TCP | DNS, DHCP, ....etc., uses UDP |

Every Computer will be assigned an IP address to identify each one to communicate in the network

Multicasting allows a single message to be sent to a group of recipients.

A subnet mask allows the users to identify which part of an IP address is reserved for the network and which part is available for host use.

A Gateway is the network point that provides entrance into another network.

|  |
| --- |
| **/etc/sysconfig/network-scripts** is the directory which contains the NIC configuration information. |
| **/etc/sysconfig/network-scripts/ifcfg-<device name>** is the file which contains the NIC configuration details. |
| **/etc/resolve.conf** is the file which contains DNS server IP and domain name location. |
| **/etc/hostname** is the hostname configuration file. |
| **/etc/hosts** is the file which contains the local DNS server IP address. |

**Bonding or Teaming or Bridging:**

Collection of multiple NIC cards and make them as single connection (virtual) NIC card is called bonding.

There are 3 types of backup in Bonding or Teaming.

(a) Mode 0 -----> Round Robbin

(b) Mode 1 -----> Activebackup

(c) Mode 3 -----> Broadcasting

**How to assign the static IP address to the NIC card?**

**In RHEL - 6 :**

# setup

**What is the command to check all the open ports of your machine?**

#nmap localhost

**31. What is the command to check all the open ports of remote machine?**

# nmap <IP address or hostname of the remote system>  
**32. What is the command to check all the listening ports and services of your machine?**

**#**netstat -ntulp **33. How can you make a service run automatically after boot?**

**#** chkconfig <service name> on   
**What is a 3 way handshake protocol? Give an example of it.**

SYN - system 1 sends SYN signal to remote system.  
 SYN-ACK - remote system receives the syn signal and sends ack signal

**How to troubleshoot if the network is not reaching?**

(i) First check the network cable is connected or not by **# ethtool <NIC device name>** command. if connected then check the IP address is assigned or not by **# ifconfig <NIC device name>** command.

(ii) Then check the system uptime by **# uptime** command.

(iii) Then check the network services status by **# service network status** and **# service NetworkManager status** commands.

(iv) Then check the network service at Run Level by **# Chkconfig --list network** command.

(v) Then check whether the source network and destination network are in the same domain or not.

(v) Then finally check the routing table by **# route -n** command.

ACK - system again receives ack signal from remote system and connection is established

# ethtool <NIC device name> (to check the network cable is connected or not)

# miitool <NIC device name> (It is also used to check the network cable but it works on

# netstat -r (to check the default gateway and routing table)

# route (to check the default gateway with routing table)

# ip route (to display the NIC device with default gateway)

**SELinux?**

It is a one type of security that enhances the security that allows users and administrators more control over which users and applications can access which resources, such as files, Standard Linux access controls etc.,

We can implement the SELinux mainly in 2 modes.

(i) Enabled

(ii) Disabled (default mode)

# vim /etc/selinux/config -----> It is main file for SELinux.

# getenforce (to check the SELinux mode)

# setenforce 0 or 1 (to set the SELinux mode

In Linux systems the booting is done in 6 stages.

* BIOS
* MBR
* GRUB
* Kernel
* Init
* Runlevel

BIOS stands for Basic Input and Output System. This process is called POST (Power On Self Test) . So, in simple terms the BIOS loads the MBR into memory and executes the MBR.

**MBR :**

MBR stands for Master Boot Record,IPL,PTI,Bootloader

simple terms the MBR loads and executes the GRUB boot loader

**GRUB or LILO :**

GRUB stands for Grand Unified Boot loader GRUB configuration file is **/boot/grub/grub.conf** (**/etc/grub.conf** is a link to this). . LILO stands for Linux Loader and is used in old Linux systems This file contains kernel and initrd images. So, in simple terms GRUB just loads and executes kernel and initrd images

**Kernel :**

Kernel initialises itself and loads the kernel modules and mounts the root file system, specified in the "root=" in grub.conf and then kernel executes the **/sbin/init** program

**init level :**

In this init program reads the **/etc/inittab** file and put the system into specified run level

**Run Level Programs :**

The following run levels are available in Linux systems.

* 0 -----> halt or shutdown the system
* 1 -----> Single user mode
* 2 -----> Multi user without NFS
* 3 -----> Full multi user mode but no GUI and only CLI mode
* 4 -----> Unused
* 5 -----> Full multi user mode with GUI (X11 system)

6 -----> reboot the system

# who -r (to see the present run level of the system)

**How to change the default run level?**

First open the **/etc/inittab** file by **# vim /etc/inittab** command and go to last line change the run level number

**# reboot** command will not send the kill signals to the system and it will kill all the running processes and services forcefully and then restart the system.

**# init 6** command will send the kill signals to the system and it will stop all the processes and services one by one and then restart the system.

**What is console port and how to connect to the console port?**

Console port is used to connect the system even though the system is not booted with the main O/S. This port is used to connect the system for troubleshooting purpose only. We can connect the console port as same as connect to systems LAN port and it is also having IP address, user name and password to connect to the console

**System is continuously rebooting. How to troubleshoot it?**

1. Connect the system through console port through putty by providing IP address, user name and password.

(v) If RAM module is not working the system get panic and it may continuously reboots.

1. (vi) If the RAM module is working then check the RAM size whether the sufficient RAM that requires to run the application is available or not.

**How to repair the corrupted boot loader and recover it?**

1. This problems may be occur if the GRUB is corrupted. So, we have to recover the GRUB. Basically the repairing of GRUB means installing the new grub on the existing one from RHEL - 6 DVD. The steps are given below.

The drivers is Linux system are known as Modules or Kernel Modules. These modules are assigned by kernel depending on the hardware

# lsmod (to list all the currently loaded modules)

# modprobe -r <module name> (to remove the specified module

**What is** " **wait** " **and where it is stored?**

(i) If there is not enough memory to run the process, then it will wait for free space in memory. That process is called wait.

(ii) wait is stored in buffer like cache memory.

cron jobs are scheduling jobs automatically at a particular time, day of the week, week of the month and month of the year.

* **/etc/crontab** -----> is the file which stores all the scheduled jobs.
* **/etc/cron.deny** -----> is the file used to restrict the users from using cron jobs.
* **/etc/cron.allow -----**> is used to allow only users whose names are mentioned in this file to use cron jobs and this file does not exist by default.

Through ssh we can connect the remote host by two methods.

* (i) Command Line Interface (CLI).
* Example : # ssh <IP address of the remote system> (provide login name and password)
* (ii) Graphical User Interface (GUI).
* Example : open VNS server window and provide remote hostname, login name and

**In how many ways we can connect the remote system?**

* (i) telnet (ii) ssh
* (iii) rlogin (iv) rcp
* (v) ftp (vi) scp
* (vii) sftp (viii) tftp

**ssh with keybased authentication**

executing **# ssh-keygen**

**/home/<user name>/.ssh**

**id\_rsa** (private key) and **id\_rsa.pub** (public key).

**# ssh-copy-id -i <user name>@<IP address of the remote system>**

**# cat /home/<user name>/.ssh/authorized\_keys** file

**How to prevent the remote login ?**

**# vim /etc/ssh/sshd\_config PermitRootLogin yes**

**allow empty password through ssh?**

**# vim /etc/ssh/sshd\_config**

**PermitEmptyPassword no**

**to prevent the password authentication mechanism in ssh?**

**PasswordAuthentication no**

**How to allow or deny the uses or group to access the remote systems through ssh?**

DenyUsers <user 1><user 2><user3> ...etc., (these users will be denied the ssh service)

AllowUsers <student><user 4><user 5> ...etc., (these users will be allowed the ssh

**How allow the specified no. of users to access remote system at a time?**

**# vim /etc/ssh/sshd\_config**

**MaxAuthTries <no.>**

**How to allow or deny the hosts or networks to use the ssh?**

**To deny IP addresses or hostnames :**

(i) Open **/etc/hosts.deny**file by **# vim /etc/hosts.deny** and go to last line and type as,

**sshd: <IP address 1**>**<IP address 2**><**IP address 3>** ...etc., (to deny IP 1, IP 2, IP 3, ...etc.,)

**sshd: <hostname 1**>**<hostname 2**><**hostname 3>** ...etc.,

# nmap -p 22 <IP address of the remote host> (to see the ssh is running or not on remote system)

**How to troubleshoot if the client has complain that I am not accessing the server using ssh?**

First check the pinging of the client system, ) Check the client <IP address or hostname> in **/etc/hosts.deny** files

# scp <source file name with full path><IP address of the remote system>:<destination location>

**rsync** is a very good program for backing up or mirroring a directory tree of files from one machine to another machine and for keeping the two machines " **in sync** ".

Swap space in Linux is used when the amount of the Physical memory (RAM) is full.

Yes, swap space is compulsory to be created at the time of installation. But additional swap space can be created and deleted at any point of time, when it is required

(i) By creating a new swap partition on the disk. (separate swap partition)

(ii) By creating swap file.

The combination of Physical memory (RAM) and swap space is called the virtual memory.

So, Virtual memory = Physical memory (RAM) + swap space.

**What happens when the /usr is full?**

(i) Users cannot login to the system.

(ii) If already login users not able to execute any command.

**/etc/yum.conf** -----> is the yum configuration file.

**/etc/yum.repos.d** -----> is the directory which contains the yum repository configuration file.

**/etc/yum.repos.d/xxxxx.repo** ------> is the yum repository configuration file.

**/var/lib/yum** -----> is the directory which contains the yum databases.

**/var/log/yum.log** -----> is the file which stores the yum log messages.

**/etc/yum.repos.d**

name=yum repo server (yum server name)

baseurl=file:///var/ftp/pub/rhel6 or baseurl=ftp://<IP address of the system>/pub/rhel6

gpgcheck=0 (0 means while installing it will not ask any signature keys of yum packages, If it is 1, then it will ask the signature keys while installing the packages)

+98u enabled=1

Copying files from local disk to any removable media is called backup.

Copying files from any removable media to local disk is called recovery or restore

**Platform Backup Tools**

Windows ntbackup

Linux tar, cpio, dd, dump, restore

3rd party Veritas netbackup, Amanda and Tivoli

cpio means copy input and output. It supports any size of the file system. It skips the bad blocks also.

# ls <source file name> |cpio <options>><destination file name>

dd means disk to disk backup. Using dd command we can take a backup of the data from one disk to another disk

# dd if = <disk 1> of = <disk 2>

dump is a command used to take a backup of file systems only. We cannot take a backup of files and directories.

so, first install the  **dump** package and then execute the dump commands.

# dump <options><destination file name><source file name>(to take a backup of the file systems)

# dump -0uvf /opt/full.dump /coss (to take a full backup of the /coss file system and copied it in /opt)

# dump -1uvf /opt/full.dump /coss (to take a backup modified files from the last full backup nothing but incremental backup)

# restore <options><dump backup file> (to restore the backup contents if that data is lost)

# restore -tf /opt/full.dump (to list the dump file contents)

# restore -rf /opt/full.dump (to restore the dump file contents)

There are mainly three types of backups available.

(i) Full backup (Entire file system backup)

(ii) Incremental backup (backup from the last full backup or incremental backup)

(iii) Cumulative or differential backup (backup from last full backup or cumulative backup)

**/etc/dumpdates** file will be updated when backing up with dump command

The point - in - time copy of the file system is called the snap shot.

(i) Normally in backup environment we have 3 servers.

(a) Master server (production servers -- 1 or 2 no's).

(b) Media server (backup server -- 1 or 2 no's).

(c) Client server (Normal system)

(ii) Backups can be taken in types.

(a) Application Backup (Normally application users will take these types of backups)

(b) File system Backup (O/S backup, System Administrators will take these types of backups)

(c) Database Backup (DBA users will take these types of backups)

(iii) Normally backup is automated through some backup tools like Veritas Net backup, IBM Tivoli and Autosys.

By dump command we can take backups on disks, tapes and takes full, incremental and differential or cumulative backups.

(ii) level 0 -- Full backup (monthly once)

level 3 -- Performed on every Monday (Incremental from last full or last incremental backup)

level 4 -- Performed on every Tuesday (Incremental from last level 3 backup)

level 5 -- Performed on every Wednesday (Incremental from last level 4 backup)

level 6 -- Performed on every Thursday (Incremental from last level 5 backup)

level 7 -- Performed on every Friday (Incremental from last level 6 backup)

level 8 -- Performed on every Saturday (Incremental from last level 7 backup)

level 2 -- Performed on every Sunday (differential or cumulative backup from last full backup, ie., from Monday to Saturday)

/etc/dumpdates file records the backup information if -u option is used with dump command to take a backup. In this file each line tells the file system that was backed up, last level of backup, the date, day and time of the backup.

# nice (to run a program with modified scheduling priority ie., it runs the process with an adjustable niceness)

# renice (to alter the scheduling priority of one or more running processes)

A process is a set of instructions which executes in the memory.

The first process in RHEL - 6 is **initd** and it starts at boot time. It's process ID is 1 where as in RHEL - 7 the first process is **systemd** and it starts at boot time. To manage or to see the processes there are two commands.

(i) # ps and (ii) # top

**# ps :**

It is just a snap shot of the current status of the processes. It gives only one terminal information not all the terminals information.

**# top :**

Using top command we can monitor the processes continuously. By default every 3 seconds it will refresh the data.

# ps -aux

(it displays all the terminals processes information including background processes with user names)

# ps -ef (it displays the total processes information with parent process ID (PPID))

Zombie process (the process which is running without child process and is indicated by " **Z** " ).

# nice -n <nice value range from -20 to 19><command> (to set a priority to a process before starting it)

**How to solve the issue if the CPU utilization is 99% ?**

(i) First check which process and who executed that process is consuming more CPU utilization or memory utilization by executing **# top** command.

(ii) Then inform to those users who executed that process though mail, message or raising the ticket.

(iii) If those users are not available or not responding to our mail then we have to change the priority of that process using **# renice** command.

(iv) Before changing the process priority level , we have to get or take approval from our team lead or project manager.

**# cat /proc/cpuinfo** command will show no. of CPUs, no. of cores, no. of threads, no. of sockets and the CPU architecture, ...etc., information.

**# uptime** is the command to check the system load, present time, from how many hours the system is running and load average.

**# tcpdump** is the command to capture and analyze the network traffic. By using this command we can also troubleshoot the network problems.

**How to limit the CPU usage of a linux process?**

(a) First install the **cpulimit** package by **# yum install cpulimit -y** command

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network

(ii) LDAP client configuration file is **/etc/ldap.conf**

(iii) LDAP kerberos configuration file is **/etc/krb5.conf**

(iv) sssd (systems security service deamon) deamon.

(v) LDAP port no. is 389.

DNS stands for Domain Naming System. The **DNS**translates Internet domain and host names to [IP addresses](http://compnetworking.about.com/od/workingwithipaddresses/g/ip-addresses.htm).

Any DNS query involves two parts.

(i) **The Resolver:** The resolver forms up or initiates the query. The resolver itself does not run as a program**. /etc/resolve.conf** is an example of a resolver.

(ii) **Name Server:** The Name Server is the service running in the server that responds to the DNS query generated by the resolver i.e. answers to the question of the resolver.

Like a physical address, internet domain names are hierarchical way. If the Fully Qualified Domain Name is **www.google.co.in** , the **www** is the Hostname, **google** is the Domain, **co** is the Second Level Domain and **in** is the Top Level Domain.

There are four files to edit to configure the DNS. They are **/etc/named.conf, /etc/named.rfc1912.zones,**  **Forward Lookup Zone**and **Reverse Lookup Zone**. DNS provides a centralised database for resolution. Zone

is storage databasewhich contains all the records.

**Forward Lookup Zone** is used to resolve**Hostnames** to **IP addresses**.

**Reverse Lookup Zone** is used to resolve **IP addresses** to **Hostnames.**

(i) **SOA Record :** (Start of Authority)

SOA contains the general administration and control information about the domain.

(ii) **Host A Record :**

(a) It is nothing but a**Forward Lookup Zone**.

(b) It maps **Hostname** to **IP address.**

(iii) **PTR :** (Pointer Record)

(a) It is nothing but a **Reverse Lookup Zone**.

(b) It maps **IP address** to **Hostname.**

(iv) **NS Record :** (Name Server Record)

It stores the DNS server IP addresses.

(v) **MX Record :** (Mail Exchange Record)

It stores the records of the **Mail Server IP address**.

(vi) **CNME Record :**

It is nothing but Host's Canonical name allows additional names or aliases to be used locate a system.

**What is the profile of the DNS?**

Package : **bind and caching-name**

Script : **/etc/init.d/named**

Configuration file : **/etc/named.conf and /etc/named.rfc1912.zones**

Client's configuration file : **/etc/resolve.conf**

Document root : **/var/named/**

Log file : **/var/log/messages**

Deamon : **named**

Port number : **53**

DHCP stands for Dynamic Host Configuration Protocol. DHCP is a network protocol that enables the server to assign an IP addresses to the clients in the network automatically from a defined range of IP addresses ie., scope configured for a given network.

Package : **dhcp\***

Script file : **/etc/init.d/dhcpd**

Configuration file : **/etc/dhcp/dhcpd.conf**

Deamon : **dhcpd**

Port numbers : **67 (dhcp server)** and **68 (dhcp client)**

Log messages : **/var/log/messages**

To take a backup or restore of the database first we should comeout from the database server and then take a backup or restore the backup.

(i) Exit the from the database server.

**mysql or mariadb >** exit;

(ii) Take a backup of the database.

**# mysqldump -u root -p <database name>><file name with full path>**

**Example :** # mysqldump -u root -p mydetails > /root/mydetails.bak

(iii) Delete the database from the database server.

**mysql or mariadb >drop database <database name>;**

**Example :** mysql or mariadb > drop database mydetails;

(iv) Restore the deleted database using the backup copy.

**mysql or mariadb >exit;**

**# mysql -u root -p <database name><<backup file name with path>**

**Example :** # mysql -u root -p mydetails < /root/mydetails.bak

A log server represents a central log monitoring point on a network, to which all kinds of devices including Linux or Windows servers, routers, switches or any other hosts can send their logs over network

Log file is file that contains messages about that system, including the kernel, services and applications running on it, ....etc.,

**The different types of log files and their locations :**

**/var/log/messages** -----> System and general messages and DHCP log messages.

**/var/log/authlog** -----> Authentication log messages.

**/var/log/secure** -----> Security and authentication and user log messages.

**/var/log/maillog** -----> Mail server log messages.

**/var/log/cron** -----> Cron jobs log messages.

**/var/log/boot.log** -----> All booting log messages.

**/var/log/httpd** -----> All Apache web server log messages.

**/var/log/mysqld.log** -----> Mysql database server log messages.

**/var/log/utmp** or **/var/log/wtmp** -----> All the user's login messages.

**/var/log/Qmail** -----> Qmail log messages.

**/var/log/kernel.log** -----> All kernel related log messages.

**/var/log/samba** -----> All samba server log messages.

**/var/log/anakonda.log** -----> Linux installation log messages.

**/var/log/lastlog** -----> Recent login information for all users.

**# lastlog** (to see the log messages of the above log file)

**/var/log/yum.log** -----> All package

**IPtables or firewalls?**

IP tables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. If it doesn’t find one, it resorts to the default action. IP tables almost always comes pre-installed on any Linux distribution.

There are four types of firewalls.

(i) **Packet firewalls :**

* It works atPhysical, Data Link and Network Layers.
* It works fast and efficiently.
* It treats each packet in isolation.

(ii) **Statefull firewalls :**

* It identifies a packets connection state.
* It maintains packets history in the state tables.

(iii) **Application layer firewalls :**

* It inspects and filter packets on OSI layer upto Application Layer.
* It identifies if protocols are being misused.

(iv) **Proxies firewalls :**

* It acts as an intermediary.
* It operates at Application Layer.

It won't allow direct connections

**/etc/sysconfig/iptables** is the configuration file of IP tables.

**# iptables <options><chain> firewall-rule**

There are 4 ways to protect the network.

(i) SELinux

(ii) IP tables

(iii) Firewalld

(iv) TCP wrappers

### How do you know your system has a high load?

The most important question as in most cases I have seen how do you determine your system has high load.  
 *Does a high value represents high load average and that your system requires attention?*  
 *What is the threshold value for load average?*  
 *How can we conclude if the load average value is good or bad?*   
 A Central Processing Unit in earlier days used to be having only one processor and the core concept was not their in those days. But with the advancement in technology and the [urge](javascript:void(0);) of higher speed to meet up demands of IT industry multiple processor were integrated in the same CPU making it multi-processor.  
 However [increasing](javascript:void(0);) the no. of processor did increased the working speed of many tasks and performance but it also leads to increase in size, complexity and heat issues. So, in order to continue improvement of performance the core concept was introduced.  
 Instead of having two CPUs and a motherboard capable of hosting them, two CPUS are taken together and combined to form a [dual core processor](javascript:void(0);) which will utilize an individual socket using less power and size capable of performing the same amount of task as dual processor CPU.  
 **Bottom Line** is that Load value depends on the no. of cores in your machine. For example a dual core is relevant to 2 processor or 2 cores and quad core is relevant to 4 processor or four cores as the maximum value for load.