LAB CYCLE:3

EXPERIMENT NO: 5

Date:

FILE SYSTEM HIERARCHY, PERMISSION, CONFIGURATION FILES AND LOG FILES

Aim: a) File system hierarchy in a common Linux distribution,

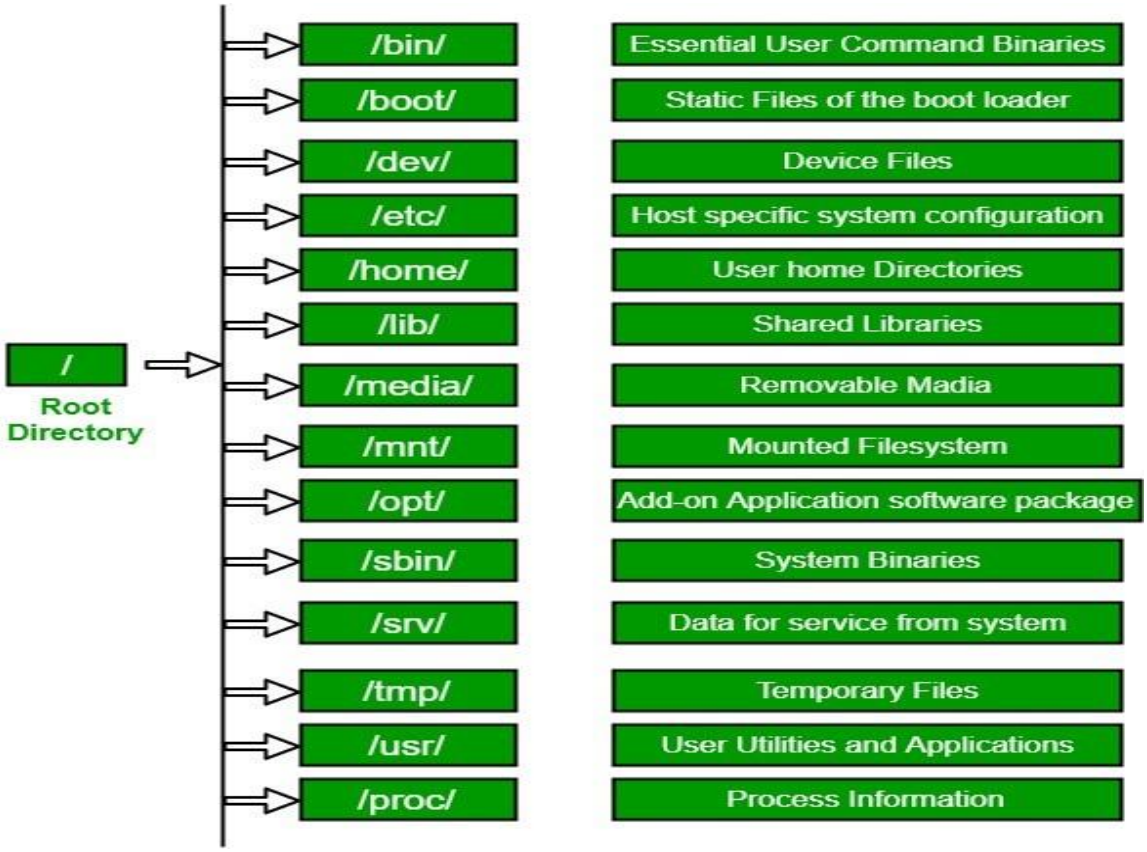
b) File and device permissions,

c) Study of system configuration files in /etc,

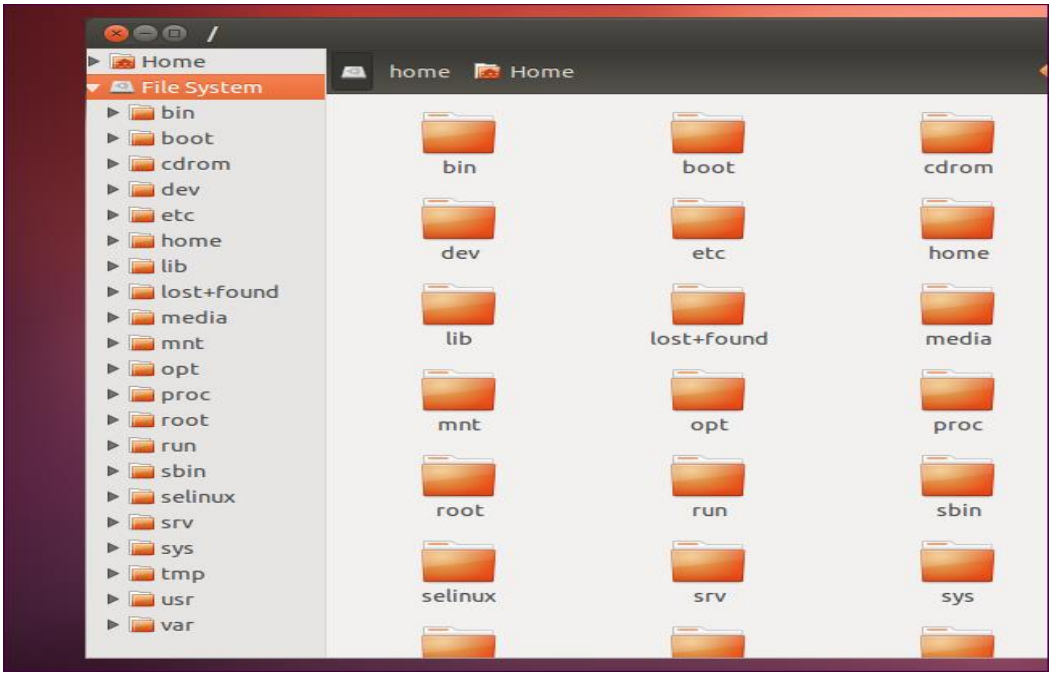
d) Familiarizing log files for system events, user activity,network events.

a) File system hierarchy in a common Linux distribution

The Linux File Hierarchy Structure or the File System Hierarchy Standard (FHS) defines the directory structure and directory contents in Unix-like operating systems. It is maintained by the Linux Foundation. In the FHS, all files and directories appear under the root directory /, even if they are stored on different physical or virtual devices.

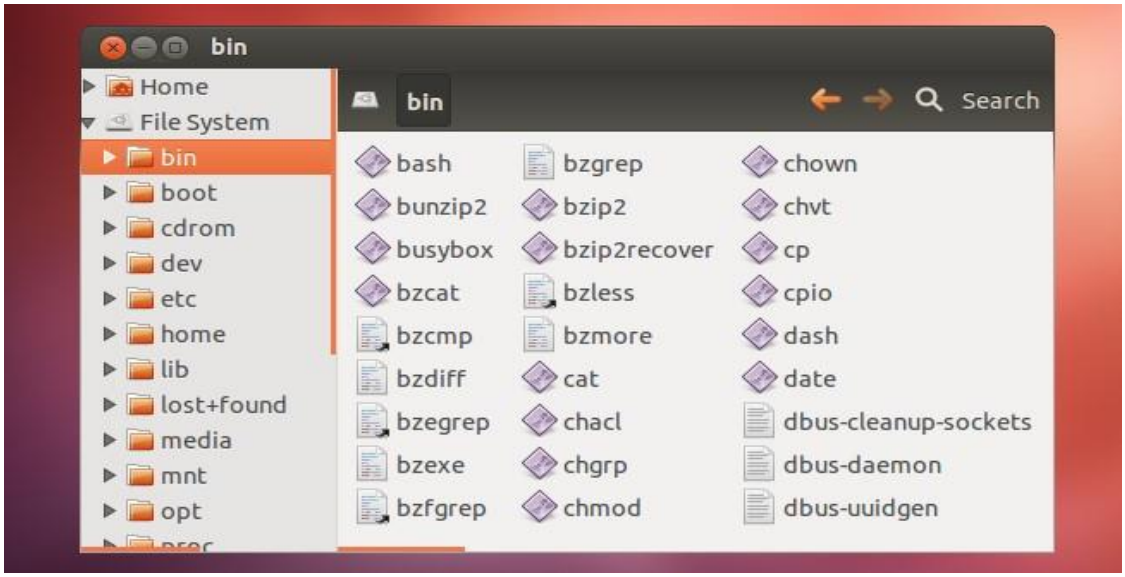


1. The Root Directory



- Every single file and directory starts from the root directory.
- The only root user has the right to write under this directory.
- /root is the root user's home directory, which is not the same as /.

2. /bin- User binaries

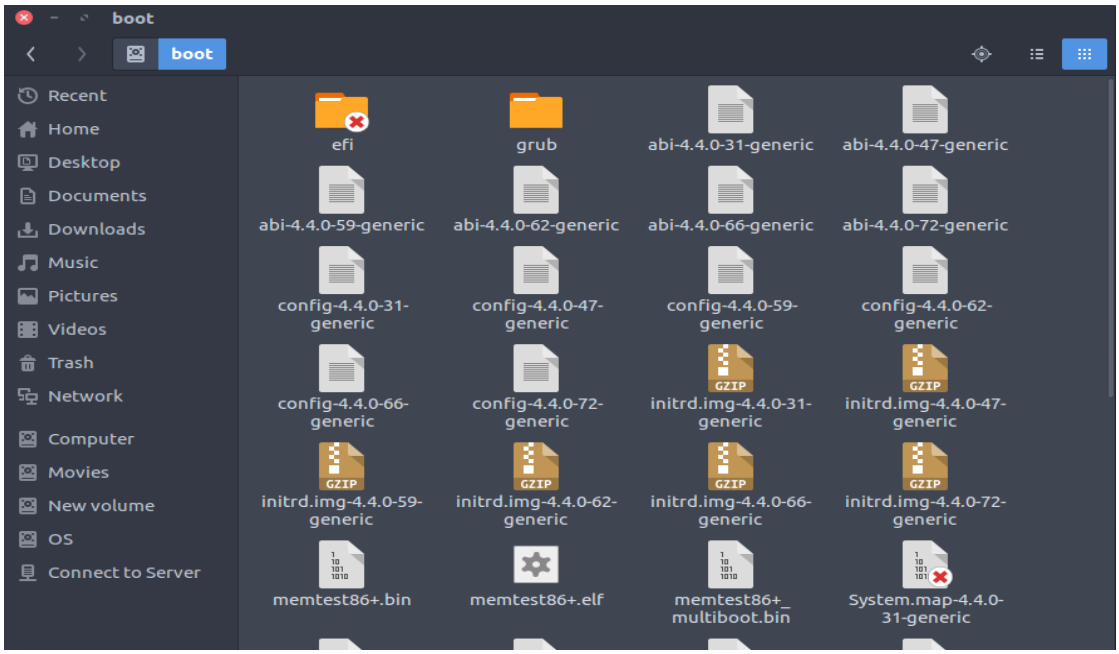


- Contains binary executables
- Common Linux commands you need to use in single-user modes are located under this directory.

- Commands used by all the users of the system are located here

  e.g. ps, ls, ping, grep, cp, cat, ls.

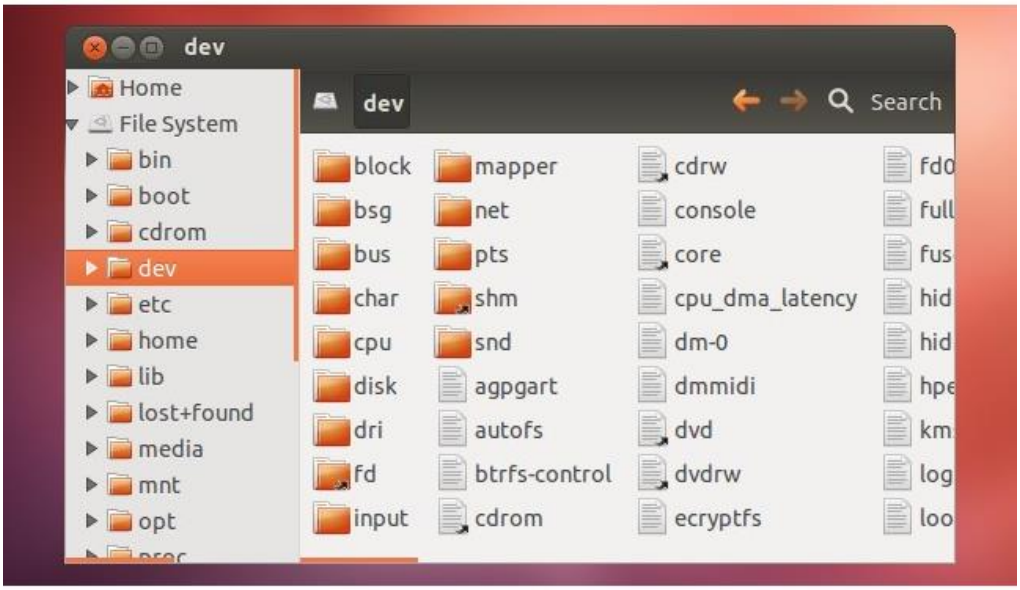
3. /boot – Static Boot Files



- Boot loader files
- Kernel initrd, vmlinux, grub files are located under /boot

  Example: initrd.img-2.6.32-24-generic, vmlinuz-2.6.32-24-generic

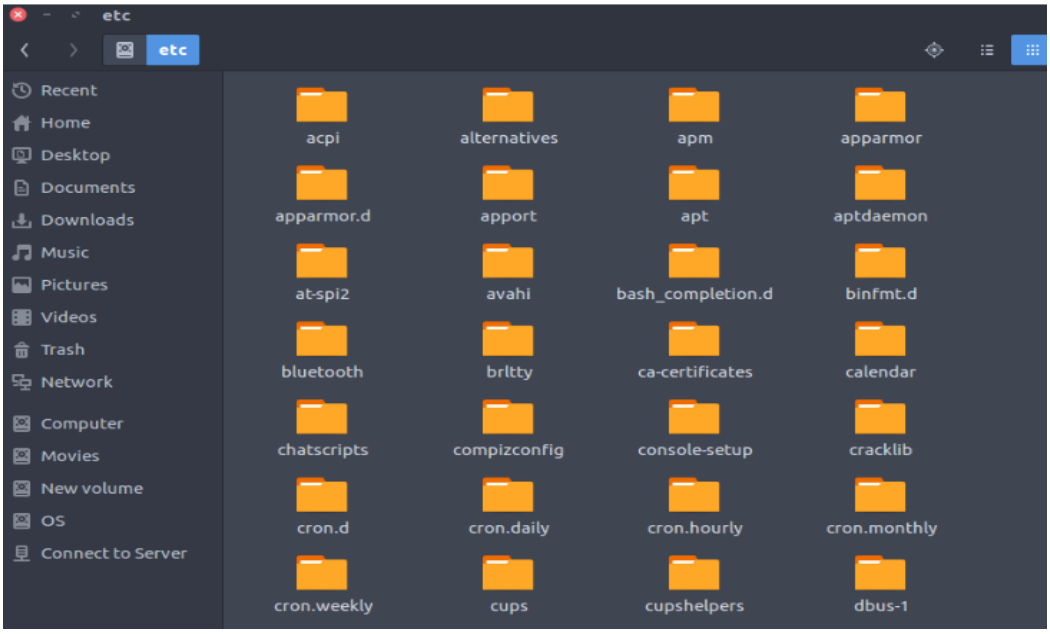
4. /dev-Device Files



- Contains device files
- These include terminal devices, usb, or any device attached to the system.

- These are not actual files as we know them, but they appear as files – for example, /dev/sda represents the first SATA drive in the system. If you wanted to partition it, you could start a partition editor and tell it to edit /dev/sda.
- This directory also contains pseudo-devices, which are virtual devices that don't actually correspond to hardware.

5. /etc- Configuration Files



- Contains configuration files required by all programs.
- This also contains start-up and shutdown shell scripts used to start/stop individual programs.

  Example: /etc/resolv.conf

b) File and device permissions

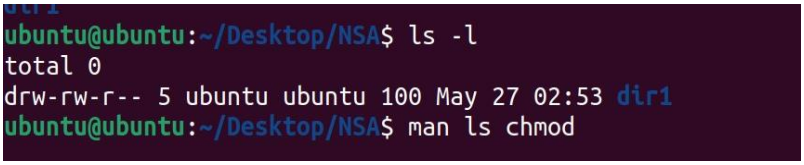
Since Ubuntu is a multi-user operating system, so it has security to prevent people from accessing each other's confidential files. When you do so, each file will be listed on a separate line in a long format.

$ls -l

1. There's a lot of information in those lines.
2. The first character = '-', which means it's a file

   'd', which means it's a directory.

3. The next nine characters = (rw-r–r–) show the security
4. The next column shows the owner of the file. (Here it is `root`)
5. The next column shows the group owner of the file.
6. The next column shows the size of the file in bytes.
7. The next column shows the date and time the file was last modified.
8. Last Column = File_name or Directory_name.



Security Permissions

rwx rwx rwx

user group other

Letters Definition

‘r’: “read” the file’s contents.

‘w’: “write”, or modify, the file’s contents.

‘x’ : “execute” the file. This permission is given only if the file is a program.

Operators Definition

`+`: Add permissions

`-`: Remove permissions

`=`: Set the permissions to the specified values

Reference Class Description

`u`(user): The user permissions apply only to the owner of the file or directory, they will not impact the actions of other users.

`g`(group): The group permissions apply only to the group that has been assigned to the file or directory, they will not affect the actions of other users.

`o`(others): The other permissions apply to all other users on the system, this is the permission group that you want to watch the most.

`a`(All three): All three (owner, groups, others)

Changing security permissions

The command you use to change the security permissions on files is called “chmod“, which stands for “change mode” because the nine security characters are collectively called the security “mode” of the file.

Adding execute permission

chmod o+x filename

Change multiple permissions at once

chmod ugo-rwx filename

Revoke execute(x) permission from others(o)

chmod ug+rw,o-x filename

Octal values

When Linux file permissions are represented by numbers, it's called numeric mode. In numeric mode, a three-digit value represents specific file permissions (for example, 744.) These are called octal values. The first digit is for owner permissions, the second digit is for group permissions, and the third is for other users. Each permission has a numeric value assigned to it:

r (read): 4

w (write): 2

x (execute): 1

In the permission value 744, the first digit corresponds to the user, the second digit to the group, and the third digit to others. By adding up the value of each user classification, you can find the file permissions.

For example, a file might have read, write, and execute permissions for its owner, and only read permission for all other users. That looks like this:

Owner: rwx = 4+2+1 = 7

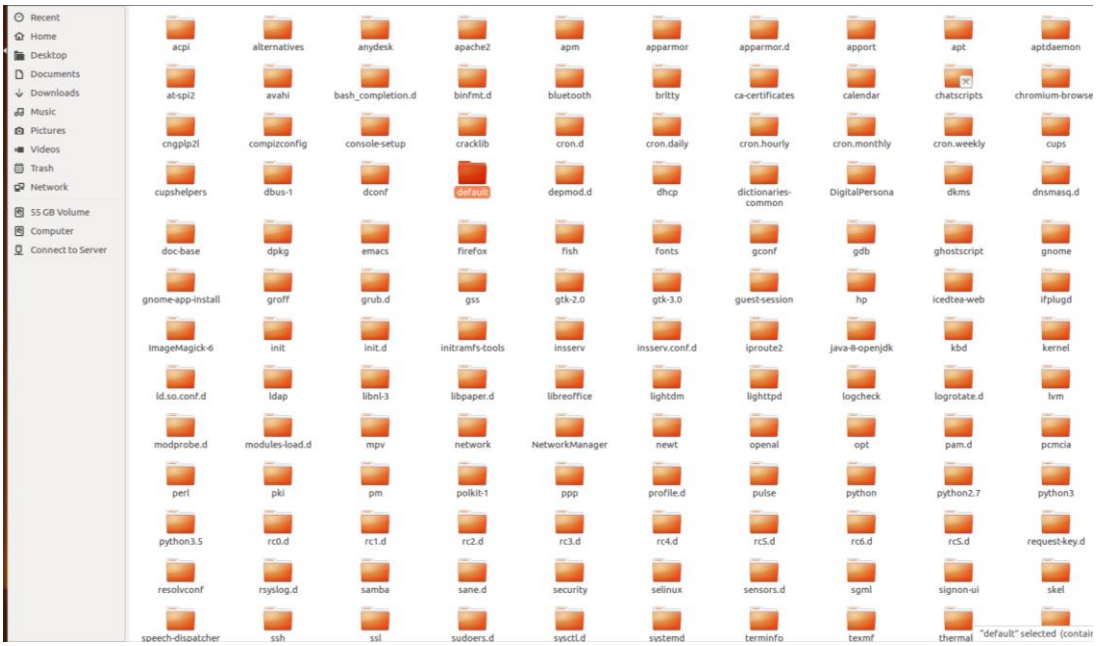
Group: r-- = 4+0+0 = 4

Others: r-- = 4+0+0 = 4

The results produce the three-digit value 744.

c) Study of system configuration files in /etc

Linux configuration files enable the Kernel to know about users, their login state, and manage file permissions and user groups. Most of the configuration files in Linux are usually under the /etc folder./etc(et-see) directory is where a linux configuration file live. The configuration files are static and cannot be executable. They are used to control the operation of various Linux programs.



Types of Configuration Files in /etc

1. Access files

2. Booting and login/logout

3. File system

4. System administration

5. Networking

6. System commands

7. Daemons

1. Access files

Access files tell the network domain how to look up host names.

Access files include:

- /etc/hosts.config
- /etc/hosts
- /etc/hosts.allow
- /etc/hosts.deny

2. Booting and login/logout

These files contain configuration information for booting up the system.

/etc/issue & /etc/issue.net

/etc/rc.d/rc

/etc/rc.d/rc.sysinit

/etc/rc.d/rc/rc X.d

3. File system

Linux provides /proc, a virtual file system that can be used to display various system data structures and parameters.

Many programs access this file system to gain statistical information about the system, such as the devices mounted on the system, the memory usage, etc.

/etc/mtab

/etc/fstab

/etc/mtools.conf

4. System administration

This group of files contains information about the users and user groups, as well as the file permissions and credentials of all users. These files include the following configuration files:

/etc/group

/etc/nologin

/etc/passwd

/etc/securetty

/etc/shadow

5. Networking

/etc/networks

Lists names and addresses of networks accessible from the network to which the machine is connected. Used by route command. Allows use of name for network.

/etc/protocols

Lists the currently available protocols

/etc/services

Translates network service names to port number/protocol.

6. System commands

System commands are meant to be used exclusively by the system. Programs like login or bash are all system commands. These are important files containing information about the system commands and include the following files.

/etc/lilo.conf

/etc/logrotate.conf

/etc/ld.so.conf

/etc/inittab

/etc/termcap

7. Daemons

Daemons are programs that run in the background without user interference.

These are often related to networking stacks, where they wait for connections to arrive so that they can provide services through them.

/etc/syslogd.conf

/etc/httpd.conf

/etc/conf.modules

d) Familiarizing log files for system events, user activity,network events.

Log files are a set of records that Linux maintains for the administrators to keep track of important events.

They contain messages about the server, including the kernel, services and applications running on it.

Linux provides a centralized repository of log files that can be located under the /var/log directory.

When issues arise, analyzing log files is the first thing an administrator needs to do.

How can Linux Log files help

1. Troubleshooting

When something goes wrong on a Linux system, logs can help pinpoint the issue.

By examining system logs, application logs, and service logs, it's possible to identify errors, warnings, and other messages that indicate what went wrong.

2. Diagnosing Performance Issues

System logs can help identify performance issues like memory leaks or disk I/O bottlenecks.

Examining application logs can also help identify performance issues with specific applications.

3. Monitoring System Health

Linux logs can be used to monitor system health and detect issues before they become critical.

By monitoring system logs, administrators can identify trends and patterns that could indicate a problem is brewing.

4. Compliance and Auditing

Many organizations are required to maintain logs for compliance and auditing purposes.

Linux logs can help organizations meet these requirements by providing a record of system activity.

5. Security

Linux logs are an essential tool for monitoring and detecting security issues.

System logs can be used to detect unauthorized access attempts, while application logs can help identify suspicious activity within specific applications.

By monitoring logs, administrators can quickly identify and respond to security incidents.

The log files generated in a Linux environment can typically be classified into four different categories:

- Application Logs
- Event Logs
- Service Logs

- System Logs

1. System Logs

These logs contain information about the system's operation, such as boot messages, kernel messages, and hardware events.

System logs are essential for troubleshooting system issues, and monitoring system performance.

2. Application Logs

These logs contain information about the behaviour of an application, including errors, warnings, and other messages.

Application logs are used to diagnose problems with applications and to analyze application performance.

3. Service Logs

These logs contain information about services running on the system, including network services and daemons.

Service logs are used to monitor service activity, and optimize service performance.

4.Event Logs

These logs contain information about events on the system, such as user logins, system shutdowns, and security events.

Event logs are used to audit system activity, track user activity, and investigate security incidents

Which Linux log files to monitor?

Monitoring and analyzing all of them can be a challenging task.

The sheer volume of logs can sometimes make it frustrating just to drill down and find the right file that contains the desired information.

1. /var/log/messages

2. /var/log/auth.log

3. /var/log/secure

4. /var/log/boot.log

5. /var/log/dmesg

6. /var/log/kern.log

7. /var/log/faillog

8. /var/log/cron

9. /var/log/yum.log

10. /var/log/maillog or /var/log/mail.log

11. var/log/httpd/

12. /var/log/mysqld.log or /var/log/mysql.log

Result:

Familiarisation with file system hierarchy,permission, configuration files and log files has been done successfully.