from harddisk to the RAM & it stick to RAM even after its execution.

enable on stickey bit on Repeatedly executable programs will speed up the execution as it avoid Reading the file from hard disk every time its executes

SGID:- when enabled on executable files the program Runs with group previlages when SGID is enabled on directories, all the child directories and files inherits the group privillages.

Note

05/01/19

- Access Control list:- Access Control list provides an additional more flexible permissions for a file system or files or directory. ACLs allow fine-grained permissions to be allocated to a file. named users or named groups as well as users and groups identified by a UID or GUID, can be granted permissions inaddition to standard file owner, group owner and other file permissions. file owner can set ACL's on individual files or directories. the file system need to be enabled with ACL option.

file system mount option for ACLs:- the file system needs to be mounted with ACL support enabled. xfs (Extended file system) file systems have a buildin ACL support. ext4 file systems created on RHEL7 have the ACL option enabled bydefault. Earlier versions may need the ACL option included with the mount Request or set in the superblock.

Eg:- vi /etc/fstab

dev name	dir	filetype	defaults,acl	0	0
/dev/sdc1	/oracle	ext4	defaults,acl	0	0

(or)

mount -o remount, acl /mountpoint

the remount option in the above command will Reload newly given mount options without the need of unmount.

viewing and interpriting Acl permissions:- 'ls -l' Command will only prints minimal ACL settings.

Ex:- ls -l xyz.txt

-rw-rw-r--+ 1 root root 34 NOV10 21:43 xyz.txt

the '+' symbol at the end of the 10th character permission indicates that there are ACL settings associated with this file.

viewing file ACL's:- To display Acl settings on a file use

getfacl filldirname.

Ex:- getfacl u.txt

file : u.txt
owner : root
group : root
flags : s-t

user : : rw-
group : : r--
Other : : r--

In the above file 1st four lines are commented, indicates file name, owner, group & flags Respectively. flags Refers to file attributes such as SetUID, SetGID and sticky bit.

user entries:-

1. the 1st user entry Refers to the file owner permission whereas Root is having r&w permission,
2. The 2nd user entry Refers the name dbadm associated with this file.

user : : rw-
named user : dbadm: rw-

group entries:- The group permission having Read access and named group loracle is having read and write access.

mask entry:- mask setting indicates the maximum possible permissions for all named users, group owner & named groups but not the file owner.

Setting up ACL's:- use setup ACL (or) Setfacl Command to add, modify or Remove standard ACL's on files and directories

Syntax:- Setfacl -m u:username:rwx / g:groupname:rwx file/directory

Setfacl -R -m u: username directory
↓ g: group
Recursive o: other

Setfacl -d -m u: username: rwx directory
↓
default

usually default acl's are applied on directory.

Example: touch mysample.txt
ls -l
Setfacl -m u: Sample1: rwx mysample.txt
getfacl mysample.txt

Setfacl -m u: sample2: rw-, g: hr: r-x, g: fin: --- mysample.txt
getfacl mysample.txt

getfacl

Note:- Chmod command has no effect on any group permissions for files with ACL settings, but it updates the ACL mask.

To add or modify other ACL:- ACL's other and standard other permissions are Equilant, so using chmod on other permissions is Equilant to using 'setfacl' on other options.

Eg:- setfacl -m o::rw- xyz.txt

(or) chmod o=rw- xyz.txt

We can add multiple entries via same command by using comma seperation for each entry.

Eg:- setfacl -m u:sample2:rw-, g:hr:r-x, g:fin:-, o::- mysample.txt

The above command will set named user sample2 with rw- & named group hr with r-x, & named group fin with no permissions and others also with no permissions.

The ACL mask:- The ACL mask defines the maximum permissions that can be granted to named users, group owner, and named groups. It doesn't Restrict the permission of the file owner or other users. All files and directories that implement ACL's will have an ACL mask.

The mask will be calculated and added automatically if it not explicitely set. The mask also get inherited from the parent directory if a default mask is set.

default ACL entries:- The default ACL can be applied on owner, named user, group owner and a named group. The file owner will get the file permissions as narrated below. ~~the default owner~~ the named user will obtain read & write on a permissions for files created in the directory & Read, write & execution permission for directory created in the directory.

Ex:- mkdir sap

cd sap

touch x.txt

ls cd

ls -ld sap

setfacl -d -m u:sampul:rwx, g:tin:rwx sap

ls -ld sap

getfacl sap

cd sap

touch x.txt

ls -l

getfacl x.txt

mkdir subdir

ls -l

getfacl subdir/.

Removing all ACL setting for file or directory:-

Syntax:- setfacl -b filedir

↓

Removes all ALC's onto of given filedir.

Removing default ACL:-

Syntax:- setfacl -k filedir.

Removing specific ACL entry:-

Setting a ACL's of one file to another:-

Syntax:- getfacl x.txt > acl.out

setfacl --set-file=acl.out y.txt

getfacl y.txt

touch z.txt

setfacl --set-file=acl.out z.txt

(or)

getfacl x.txt | setfacl --setfile= - m.txt

modifying or changing ACL's with set- option:-

you can use --set (or) --set-file options to set ACL's of a file/directory. The output from getfacl can be used as a input to setfacl command

Eg:- getfacl x.txt | setfacl --setfile:- m.txt.

the --set-file option accepts input from a file (or) stdin, and the '-' (hypen) specifies the use of stdin. in the above case m.txt will have same ACL's as x.txt.

storing ACL's into a file:-

Syntax:- getfacl filename > acloutfile

apply the above created file on some other file as below

setfacl --set-file=file = acl.out file/dir.

deleting an ACL:- deleting specific ACL

setfacl -x u:username:permission filename

TO remove all ACL's setfacl -b file/dir

1. Create group called 'sodor'

Create a user called James

Create a group called a) bakerstreet b) scotlandyard.

create users lesttrade, gregson, Jones as part of scotlandyard.

Create users holmes, watson as part of baker-street.

a) add named ACL's to the steamies directory and all of its contents

i) grant the sodor ground read, write & conditional execute permissions.

ii) update steamies directory, denying the user james from the sodor group any access.

b) add named ACLs as default ACL's to support future file & directory additions.

c) add default access Rule for the sodor group, grant read, write & executed permissions on the steamies directory.

d) and add default access Rule for the user james. deny all access to the steamies directory.

2. the Baker street detective agency is setting up a collaborative share directory and copy some files into it. to hold case files which members of the bakerstreet group will have read & write permission on.

the lead detective, sherlock Holmes, has decided that members of the scotlandyard group should also be able to read & write to the shared directory. However, Holmes thinks that inspector peter Jones (a member of the scotlandyard group) is an imbecile, and as such Jones should have his access to the directory Restricted to Read only.

mrs. Hudson has limited linux skills and was only able to create

groupadd sodor.

groupadd bakerstreet

groupadd scotlandyard

useradd James, useradd Jones, useradd lestrade, useradd gregson, useradd Holmes, useradd watson.

mk dir

groupmems -a lestrade -g scotlandyard.

" " gregson -g "

" " Jones -g "

mkdir steamies

getfacl sodor

groupmems -a James -g sodor

setfacl -d -m g:sodor:rwx steamies

setfacl -d g:sodor:rwx steamies

setfacl -d -m g:bakerstreet:rw share

" " " g:scotlandyard:rw share.

Setfacl -d -m u:Jones:r-- g:scotlandyard share

Setfacl -d -m u:Jones:r--, g:bakerstreet:rw-, g:scotlandyard:rw- share

getfacl share

cd share

mkdir cases.

cd cases

touch adventure.txt, moriory.txt

ls -l

getfacl

passwd lestrade Set Redhat passwd

" gregson " " "

" Jones " " "

" Holmes " " "

" watson " " "

ls -l

check getfacl shares cases/

06/01/2019

Su Command:- Switch user also known as substitute user.

Syntax:- su username

(or)

su - username

(or)

su - (or) su

su -c Command username

su -c whoami dbadm.

when '-' is used along with su command (su - dbadm) make the shell, clears all environment variables except for term (terminal), initializes home, shell, user, logname and path.

when -c is used (su -c command username) passes a single command to the shell.

observation:-

x=100
export x
echo $x
output 100
su dbadm
echo $x
output 100

echo $x
100
su - dbadm
undefined variable.

The best practice is to use su - username where certain environment variables will be applied.

Observation:- #whoami

root

#who am i

root pts/2

su dbadm

whoami

dbadm

who am i

root pts/2

exit

su - dbadm

whoami

dbadm

who am i

root pts/2

difference between su and su- ?

mounting a dvd DVD:-

device name

Syntax: mount -o ro /dev/cdrom /mountpoint

option readonly

(or)

mount -o ro -t iso9660 /dev/cdrom /mountpoint

Type

To unmount dvd umount /mnt

Sudo Command :- (ebzidik language) sudo su -

what are the permissions of /etc/sudoers

-r-- r----

what and all users scenarios you have faced on your project?

user limits:- ulimit

- Configuration file : /etc/security/limits.conf.

the /etc/security/limits.conf file contains Stanza's that specify the process Resource limits for each user. (or) a group. each line describes a limit for a user in the form <domain> <type> <item> <value>

where <domain> can be 1. username.
2. groupname, @group syntax (% can be also used).
3 The wildcard * for default entry.

<type> can be 1. soft -
2. hard. - maximum limit for the soft limit.

<item> can be 1. core - limits the core file size (KB) - Kilobyte
2. data - max data size in KB
3. fsize - max file size in KB.
4. nofile - max no. of opened file descriptors
5. rss - max resident set size
6. cpu - max cpu time in minutes
7. nproc - max no. of processes etc.

<value> can be value Refers the associated value to limit the user.

use a value of '-1' is used to set a resource to unlimited.

```
ulimit -a
```

ulimit -f 1024

```
ulimit -f
```

1024

ulimit -f unlimited

df -i

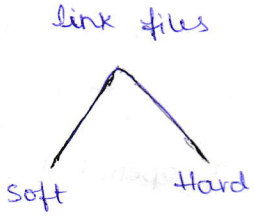
ls -li

stat <file>

1. what is file system structure?
2. what is superblock?
3. what is inode & what it consists of?
4. How will you print inode info? ls -li
5. Can you change no. of inodes of a filesystem?
6. How will you print a file inodes of filesystem.
7. What happens if I run mkfs cmd?
8. what are datablocks & why we need to have datablocks?
9. Why only 4KB for datablocks?
10. what ls -l command do?

07/01/19

link files: ln <file> link/<file> → ln file target



hard link cannot be allowed for hardlink directory.

It can allow only files but in directory it consists of two links (.) & (..)

(..) Refers to parent directory and

(.) Refers to current directory.

ls -lia

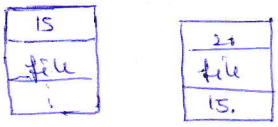
* How will you manipulate your inode numbers?
* How many (max) links you can create? (for a file) $2^{32}-1$ if it is 32 bit file system

Have you ever tried NO.

ln -f if the file is already exists it will be overwritten

Soft link:- Syntax:- ln -s link3 Slink1

ls -li = Slink → link3



directory link is only possible with softlink.

hard link can't be done across file system.

Hard link:- Syntax:- ln (already existed) source file target file → new file.

Eg:- ln x.txt y.txt.

more than one file can be Referenced by a same inode number and these files said to be hard linked each other.

directory as a file is just an array of filenames. where a directory is created it initially populates filenames (. and .. special files).

the . is a file that maps with the current directory.

.. maps to the parent directory.

softlink:-

Syntax:- ln -s source file target file.

A softlink is a file which contains the name of other file.

→ List of files opened on filesystem.

Syntax:- lsof /datafs01. → lsof /mount point name

Scenario:- when admin is trying to unmount the filesystem we will get device is busy the Reason for the same is programs/applications/database/users might be using the filesystem and hence the filesystem is busy. To solve the problem you need to examine which processes or which user using the file system below are the Commands are using same.

i) fuser- fuser identifies processes using files or sockets.

fuser -u -k /fs01

↓

kill all process used by given file system

(You need to have proper approvals to kill programs/daemons etc under the given filesystem)

2. lsof → list opened files

Syntax:- lsof /fs01.

lsof prints the open files processes along with their pids which can be killed to you unmount along the filesystem however as being it is a destruction activity makesure approval from business/client / application owner.

file system consistency check:- fsck is used to check filesystem consistency it cannot check if the filesystem is mounted

Syntax:- fsck /dev/datvg/datvol.

Note:- donot Run fsck on mounted file system.

e2fsck -n /mntpnt or /dev/vg/lv

↓

donot correct issue.

ANSWER: NO

e2fsck -y /mntpt or /dev/vg/lve

↓

yes

filesystem Journeling:- A special area on the filesystem is Reserved to keep filesystem Transactions is known as Journel.

If any abnormal unmount of a filesystem or powercutage etc. will cause filesystem corruption. in this case the Journel will be replayed to complete the filesystem Transactions.

difference between ext2, ext3, ext4?

ext2	ext3	ext4
1. There is no Journel feature available	1. Journel feature available	1. Journel feature available along with multiblock allocation
2. max file size (individual) = 16GiB to 2TB max. FS size = 2TB to 32TB	2. max. individual file size = 16GiB to 2TB But FS size can be 2TB to 32TB	2. max. file size = 16TB max FS size = 1EB (1 Exa byte = 1024PB)
3. supported from	3. Supported from kernel ver: 2.4.15	3. supported from 2.6.19 onwards
	4. Can have 32000 max subdir	4. 64000 max. subdir
		5. performance Reliability is more compared to ext3

Converting ext2 to ext3:- If you are upgrading /dev/datvg/dlv i.e., mounted on /home, to convert ext2 to ext3 do the following:-

1. umount /dev/datvg/dlvol (or) umount /oracle
2. tune2fs -j /dev/datvg/dlvol creating Journel. this will add a Journel.
3. use below command to check which filesystem.

   file -sL /dev/datvg/dlvol.

4. and again mount the device

Note:- you Really don't need to unmount while converting ext2 to ext3, it can happen dynamically

Converting ext3 to ext4:- when file system is mounted (dynamically). however it is Recommended to doing the conversion of the line.

Converting ext3 to ext4:-

1. umount /oracle.

* differences phases of ~~filesyste~~ fsck ?

when we run fsck below are the phases:-

1. pass 1 - checking inodes, blocks & sizes

pass 2 - " directory structure

pass 3 - " " Connectivity

pass 4 - " reference counts

pass 5 - " group summary information.

Process priority:-

ps -e shows all the entin process.

ps -e | more shows page by page

Every process is identified by unique id starts with '1'.

ps

PID	TTY	TIME CMD
↓	↓	↓
processid	Teletype	cpu Time (sys + user)
3512	pts/0	00:00:00 bash. → processname/command.

? means not started by any terminal.

Zombie or defunct process Represented by 'Z'. it is a process that has completed its execution but still have entry in process table.

F	S	UID	PID	PPID	C	PRI	NI	ADDR	SZ	WCHAN	STIME	TTY	TIMECMD

F - flag

S - state S, R, P, T, Z (common States)

Attempting to killing zombie process will not succeed. you might be Restart System once again however zombie process may not Refers in the above.

in the above ps -elf Refers to

F - flag. flag usually an integer number whereas 'I' Refers to the state that the process has been forked but didn't execute. and '4' is used for superuser preveliages

UID - process owners user ID or name.

PID - process ID

C - CPU utilization.

PPID - Parent process ID.

PRI - priority. The priority of a process can be identified by its priority(PRI) and Nice value (NI)

There are exactly 40 different levels of Niceness a process can have.
The Nicelevels of a process Ranges from -20 to 19. By default processes inherit Nice level from its parent which is usually '0'. Higher Nice values indicates less priority, while lower nice levels indicates a higher priority.
only Root user can increase the priority of a process. and the owner of the process can lower the priority.

launching process with different priority :-

Syntax:- nice -n <nicelevel> /path/to/command.

where nicelevel can be -20 to 19.

unpreviliged users are only allowed to set a positive nicelevel (0 to 19) and only root can set a negative nicelevels

renice:- This is the command is applied on the Job that are already running. to alter the priority of a Job.

renice -n <nicelevel> path to command. PID

Eg:- nice -n -10 /home/tejaswini/shellscripts/prg10.sh

renice -n -20 4351.

renice -n 19 4351.

The find Command:- It is used to search for files on a directory hierarchy.

Syntax:- find /path -name file/dirname -print

the path is an absolute path where we suppose to search file or directory.

find /home/tejaswini -name prg1.sh -print.

Eg:- #find / -name passwd -print

/etc/passwd

The above Command attempt find passwd file on the system and print its absolute path if it finds.

2. find a file prgl.sh on /root

```
find /root -name prgl.sh -print
```

3. To print all the files on the system.

```
find / -print
```

4. To print all the files on /home/tejaswini

```
find /home/tejaswini -print
```

5. You can use shell metacharacters on find Command. Below examples shows how to find all partition devices under /dev/sdb.

```
find /dev -name sdb? -print.
```

6. find all scsi devices.

```
find /dev -name sd* -print.
```

7. To find filenames owned by user tejaswini

```
find / -user tejaswini -prin
```

8. To search files by ignoring Case sensitiveness

```
find / -iname paSSWd -print.
```

9. To find all files that are owned by given group

```
find / -group oracle -print.
```

10. To find all files or Dir owned by user id 1000

```
find / -uid 1000 -print
```

11. To find files owned by particular user and group

```
find / -user dbadmin -group oracle -print
```

12. finding files based on permissions

```
find / -perm 755 -print
```

```
find /home/shellscripts -perm 644 -print.
```

13. Searching files based on size attributes

a) find files that are 100MB in size

```
find / -size 10M -print
```

b) find files that are greater than 10MB in size

```
find / -size +10M -print
```

14. Search files based on its modification timestamp:

a) find files that are modified 120min ago

```
find / -mmin 120 -print
```

b) find files that are modified greater than 120min

```
find / -mmin +120 -print
```

c) find files that are modified less than 120min

```
find / -mmin -120 -print
```

15. Search files based on its type:

a) find all directories

```
find / -type d -print
```

b) find all Regular files

```
find / -type f -print
```

c) find all link files

```
find / -type l -print
```

d) find all block special files

```
find / -type b -print
```

16. search a file in given device

```
find / -name xyz.txt -xdev -print
```

17. find files with inode num

```
find / -inum 35968 -print
```

-xdev is given it search will happen in that device only

find /root/scripts/ -name prgl* .sh -exec mv {} /tmp/ls-l \;

find /tmp/programs -inum 651768 -exec rm -f {} \;

ls -l

It Removes particular file with the inode number.

08/01/19

gzip:- It is used to compress a file.

Ex:- gzip filename. This command creates filename.gz compressed file.

gunzip:- It is used to uncompress gzip format file

Ex:- gunzip filename.gz

How to see particular file is there or not in tar?

tar -xvf dir.tar | grep

tar
↓
gzip
↓
unzip
↓
untar.

tar Command (Tape Achive):-

Archeiving means Safeguarding of data

TAR:- tape archive

Command to archive file / directories

tar	-cvf	tarfilename	files to archive
	-xvf		
	-tvf		

Where c - Create tar file

v - Verbose (list while doing tar)

f - tar filename

x - extract file tar file

Examples:- tar -cvf. ash.tar /tarfs

1041 tar -xvf ash.tar

1046 gzip ash.tar

1051 tar -cvf /tmp/etc.tar/etc

1053 cd /tmp1

1055 tar -tvf etc.tar

1062 du -h etc.tar

1065 gzip etc.tar

1067 gunzip etc.tar.gz

Note:- we can do tar and compression by using -z flag

```
tar -cvzf aa.tar.gz /myfiledir
```

To untar in singlestep

```
tar -xzvf filename.tar.gz
```

Compressing a file:- gzip filename

filename extensions are .gz

uncompressing a file:- gunzip filename.