**Filesystem Management 2**

26. What is swap space?  
Ans. Swap space is supplement to system RAM.  
  
27. How to set up swap partition?  
Ans. Steps involved in setting up swap partition.  
Create a partition using a partitioning program (fdisk/sfdisk/parted)  
Set partition id type to 0x82.  
Create the signature on the partition using the mkswap command  
# mkswap -v1 /dev/hdb3  
Add an entry for the swap in /etc/fstab file as:  
/dev/hdb3 swap swap defaults 0 0  
Activate the swap partition using   
# swapon -a   
Check the swap partition status using  
# swapon -s  
  
28. How to create a swap file?  
Ans. Create a file as  
# dd if=/dev/zero of=swapfile bs=512 count=N  
(Where N is the file size in KB)  
Run the mkswap to create signature  
Activate the swap file with swapon command (OR) initialize it in the startup  
script /etc/rc.d/rc.local  
  
29. Why fsck used?  
Ans. fsck (filesystem check) is used to maintain filesystem consistency.  
  
30. When the system runs the fsck and which script invokes it?  
Ans. When the system boots, the rc.sysinit script runs the fsck on any filesystems  
marked for checking in /etc/fstab file. If any of these filesystems are markes as   
dirty or have data in the journal, fsck will attempt to repair them. If it succeeds,   
the filesystems will be mounted and boot process continues, else rc.sysinit will   
run sulogin and will report that fsck needs to be run manually.  
  
31. What is e2fsck command?  
Ans. fsck is a front end tool for e2fsck.  
  
32. What is journaling?  
33. Types of journals and their function?  
Ans. Ordered : This is the default and journal only meta-data  
Journaled : Journals data and meta-data  
Writeback : Journal updates are not atomic.  
  
34. Differentiate ext2 and ext3 file systems?  
Ans. ext3 filesystem supports journaling concept where ext2 does not.  
  
35. What is the function of tune2fs command?  
Ans. This is used to modify the filesystem attributes (Like converting ext2 to ext3).  
  
36. What is the function of dump2fs command?  
Ans. Provides a dump of file system information to standard out (Console). Can be   
redirected to a file.  
  
37. What is the function of debugfs command?  
Ans. This utility is used to to examine and debug an ext2 filesystem. This can also be   
used to manually verify the inode integrity and an aid to recover data.  
  
38. What is the function of resize2fs command?  
Ans. This can be used to change the size of an ext2 or ext3 filesystem.

Filesystem Management 1

1. .Name the Linux specific partition types?

Ans.

0x82 > Linux swap

0x83 > Linux

0x8e > Linux LVM

0xfd > Linux RAID auto

0x5 > Extended

0xf > Windows partition

.2. .How many partitions are supported by Linux?

Ans.

The maximum number of partitions supported by Linux kernel is:

63 for IDE drives

15 for SCSI drives

.

3. .Why partitions required?

Ans.

Separate partitions improve performance by keeping data together which reduces the disk head seek.

.

4. .What are the tools used to create or manage partitions?

Ans.

fdisk

sfdisk

parted (GNU) - An advanced partition manipulation tool (create, copy,

resize etc.)

.

5. .What is the function of partprobe?

Ans.

Reinitializes the kernel's in memory copy of the partition table.

6. .How to create a filesystem?

Ans.

The mkfs command is used to create the filesystem.

mkfs.ext2 / mkfs.ext3 > To create ext2/ext3 filesystem

mkfs.minix > minix filesystem

mkfs.msdos > MS-DOS filesystem

.

7. .What is the difference between ext2 and ext3 filesystem?

Ans.

ext3 filesystem supports journaling, where as ext2 does not.

.

8. .What is journaling?

Ans.

.

9. .What are the journaling modes supported by ext3 filesystem?

Ans.

Ordered > Journals only metadata (This is the default)

Journaled > Journals data as well as metadata

Writeback > Journal updates are not atomic, but this gives

better performance.

.

10. .How to convert an ext2 filesystem to ext3?

Ans.

Change the /etc/fstab to specify ext3 for desired filesystem(s)

Create the ext3 journal on the ext2 filesystem(s) as:

# tune2fs -j

If the kernel needs to have access to the ext3 module at boot time, create a new initial ramdisk as:

# mkinitrd /boot/initrd-.img

11. .How to connect a file system to a Linux box?

Ans. Mount command is used.

12. .How to find currently mounted and available filesystems?

Ans.

Use mount command without arguments.

.13. .Which filesystem is referred by mount when displaying mounted & available filesystems?

Ans.

When mount command is invoked without any arguments it referes to the /etc/mtab filesystem.

.14. .How to disconnect a filesystem from a Linux box?

Ans.

The umount command is used.

.15. .Which command is used to display information about the processes using a filesystem?

Ans. The fuser command is used.

.16. . How to display who/what is acting on a filesystem?

Ans. # fuser -v mnt\_point

.17. .How to kill all actions on a filesystem?

Ans.

# fuser -km mnt\_point

.18. .How to view all the mounted and unmounted partitions?

Ans. Use the fdisk -l command to view all the mounted and unmounted

filesystems available on your system.

.19. .How to view only the mounted filesystems?

Ans.

Use the df -k command, which shows only mounted filesystems but has the big advantage of giving you the mount points too.

.20. .What is the function of e2label command?

Ans.

With the help of e2label command a filesystem label can be written into the superblock of ext2/ext3 filesystem.

Eg:- #e2label /dev/hda3 datadisk3

Will create a label of datadisk3 on the filesystem on partition /dev/hda3.

.21. .How to display the label for a device (/dev/hdb2)?

Ans.

# e2lable /dev/hdb2

.22. .What is the function of /etc/fstab?

Ans.

This file is referenced each time the system boots to create the desired filesystem hierarchy.

.23. .What are the fields /etc/fstab containd?

Ans.

The /etc/fstab fields are:

Device > Special device/filesystem

label dev to mount

Mount\_Point > The path used to access the

filesystem

fs\_type > The filesystem type

Options > List of Options (each is

separated by a comma)

Dump frequency > Level 0 dump freq (0 = never

dump, 1 = daily &

2 = every other day)

fsck Order > 0 = ignore, 1 = first (root

should have this value),

2 to 9 = 2nd, 3rd and so on.

NFS & CD-ROM s should be ignored (i.e., value 0).

.24. How to list the ext2/ext3 filesystem attributes?

Ans. lsattr command displays file attributes

.25. .How to change the ext2/ext3 filesystem attributes?

Ans. chattr command changes the file attributes.

**Linux Questions:**

**Q.** Where are the file names stored on a file system?

**A**. The actual file names are stored in the directory file they reside in. No surprise here as pretty much everything on Linux is a file. On most Linux distributions you can either cat or edit the directory name to see the file names that are within it, e.g cat /home, or vi /home

**Q.** What is a Signal in Linux, and what signal is invoked when you use the kill command? What is the difference between kill and kill -9?

**A**. A signal is a limited form of inter-process communication used in Unix, Unix-like, and other POSIX-compliant operating systems. It is an asynchronous notification sent to a process or to a specific thread within the same process in order to notify it of an event that occurred. When a signal is sent, the operating system interrupts the target process's normal flow of execution.

The difference between invoking kill with no signal specified (which uses SIGTERM, number 15) and kill -9 is that the latter tries to kill the process without consideration to open files and resources in use.

**Q.** What is a process?

**A**. A process is an instance of an executing program. When a program is executed, the kernel loads the code of the program into virtual memory, allocates space for program variables, and sets up kernel bookkeeping data structures to record various information (such as process ID, termination status, user IDs, and group IDs) about the process. From a kernel point of view, processes are the entities among which the kernel must share the various resources of the computer.

**Q.** What are the logically divided parts of a process?

**A**. A process is logically divided into the following parts, known as segments:

\* Text: the read-only machine-language instructions of the program run by the process.

\* Data: initialized/uninitialized global and static variables used by the program;

\* Heap: an area from which memory (for variables) can be dynamically allocated at run time. The top end of the heap is called the program break;

\* Stack: a piece of memory that grows and shrinks as functions are called and return and that is used to allocate storage for local variables and function call linkage information;

**Q.** What are the process states in Linux?

**A**. Running: Process is either running or ready to run

\* Interruptible: a Blocked state of a process and waiting for an event or signal from another process

\* Uninterpretable: a blocked state. Process waits for a hardware condition and cannot handle any signal

\* Stopped: Process is stopped or halted and can be restarted by some other process

\* Zombie: process terminated, but information is still there in the process table.

**Q.** What is a Socket?

**A**. A Socket is the combination of an IP address and a port number .Based on this combination, internet sockets deliver incoming data packets to the appropriate application process or thread.

**Q**. How do you debug a running process or a library that is being called?

**A**. strace -p PID

ltrace libraryfile

**Q**. How to see a memory map of a process, along with how much memory a process uses?

**A.** pmap -x PID

**Q.** You run chmod -x /bin/chmod, how do you make chmod executable again without copying it or restoring from backup?

**A.** On Linux, when you execute an ELF executable, the kernel does some mapping and then hands the rest of process setup off to ld.so(1), which is treated somewhat like a (hardware backed) interpreter for ELF files, much like /bin/sh interprets shell scripts, perl interprets perl scripts, etc. And just like you can invoke a shell script without the executable bit via ’/bin/sh your\_script’, you can do:

/lib64/ld-linux-x86-64.so.2 /bin/chmod +x /bin/chmod

**Q.** Explain the TIME\_WAIT state in a TCP connection, as displayed by netstat or ss.

**A.** A TCP connection is specified by the tuple (source IP, source port, destination IP, destination port). The reason why there is a TIME\_WAIT state following session shutdown is because there may still be live packets out in the network on its way to you. If you were to re-create that same tuple and one of those packets show up, it would be treated as a valid packet for your connection (and probably cause an error due to sequencing). So the TIME\_WAIT time is generally set to double the packets maximum age. This value is the maximum age your packets will be allowed to get to before the network discards them. That guarantees that, before your allowed to create a connection with the same tuple, all the packets belonging to previous incarnations of that tuple will be dead. That generally dictates the minimum value you should use. The maximum packet age is dictated by network properties, an example being satellite lifetimes are higher than LAN lifetimes since the packets have much further to go.

**Q.** What is Huge Pages in Linux and what use is there for them?

**A.** Hugepages is a mechanism that allows the Linux kernel to utilize the multiple page size capabilities of modern hardware architectures. Linux uses pages as the basic unit of memory, where physical memory is partitioned and accessed using the basic page unit. The default page size is 4096 Bytes in the x86 architecture. Hugepages allows large amounts of memory to be utilized with a reduced overhead.

To check: cat /proc/sys/vm/nr\_hugepages.

To set: echo 5 > /proc/sys/vm/nr\_hugepages

**Q.** What is a Master boot Record and how do you back it up and restore it?

**A.** The MBR is a 512 byte segment on the very first sector of your hard drive composed of three parts: 1) the boot code which is 446 bytes long, 2) the partiton table which is 64 bytes long, and 3) the boot code signature which is 2 bytes long.

To backup: dd if=/dev/sda of=/tmp/mbr.img\_backup bs=512 count=1

To restore: dd if=/tmp/mbr.img of=/dev/sda bs=512 count=1

**Q.** Your server is using a lot of cached memory. How do you free it up short of rebooting?

**A.** Kernels 2.6.16 and newer provide a mechanism to have the kernel drop the page cache and/or inode and dentry caches on command, which can help free up a lot of memory.

To free page cache, dentries and inodes: echo 3 > /proc/sys/vm/drop\_caches

**Q.** How do you track new concurrent connections?

**A.** Concurrent connections are the number of authenticated "handshakes" between a client and/or server during any given time before all communications have been disconnected whether by force or by refusal. You can run:

modprobe ip\_conntrack

conntrack -E -e NEW

**Q.** What is SYN flood and how can you detect it and mitigate it?

**A.** A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Detection can be done by by netstat or ss and filtering for SYN-RECV connection states. Mitigation can be done by null-routing the offending IP and enabling SYN cookies in the kernel, which allow the server to sends back the appropriate SYN+ACK response to the client but discards the SYN queue entry.

ss -a | grep SYN-RECV | awk '{print $4}' | awk -F":" '{print $1}' | sort | uniq -c | sort -n netstat -antp | grep SYN\_RECV|awk '{print $4}'|sort|uniq -c | sort -n

**Q.** You have a file with 2000 IP's. How do you ping them all using bash in parallel?

**A.** echo $(cat iplistfile) | xargs -n 1 -P0 ping -w 1 -c 1

**Q.** What command can you use to send unsolicited ARP updates to the neighboring servers' caches.

**A.** arping -U -c 1 -I eth0 0.0.0.0 -s IP\_ADDRESS

**Q.** What Linux utility can craft custom packets, like TCP SYN packets and send them to a remote host?

**A.** hping3 -S 192.168.1.1 -p 80 -i u1

**Q.** What is Memory Overcommit in Linux?

**A.** By default, Linux will allow processes to allocate more virtual memory than the system actually has, assuming that they won't end up actually using it. When there's more overcommited memory than the available physical and swap memory the OOM-killer picks some process to kill in order to recover memory. One reason Linux manages memory this way by default is to optimize memory usage on fork()'ed processes; fork() creates a full copy of the process space, but in this instance, with overcommitted memory, only pages which have been written to actually need to be allocated by the kernel.

**Q.** What is system load averag as displayed by uptime?

**A.** Load Average is the sum of the number of processes waiting in the run-queue plus the number currently executing.If there are four CPUs on a machine and the reported one-minute load average is 4.00, the machine has been utilizing its processors perfectly for the last 60 seconds.

**Q.** How do you list all kernel modules that are compiled in or enabled?

**A.** You can execute:

cat /boot/config-$(uname -r)

**Q.** What is the difference between Active and Passive FTP sessions:

**A.**

Active FTP :

command channel : client port above1023 connects to server port 21

data channel: client port above 1023 is connected from server port 20

Passive FTP :

command channel: client port above 1023 connects to server port 21

data channel: client port above 1023 connects to server port above 1023

**MySQL Questions:**

**Q.** What are the two main MySQL storage engines, and how they differ?

**A.** The two most popular storage engines in MySQL are InnoDB and MyISAM

InnoDB supports some newer features like transactions, row-level locking, foreign keys. It's optimized for read/write high volume operations and high performance.

MyISAM is simpler and better optimized for read only operations. It has limited feature set as compared to InnoDB.

**Q.** What to consider when setting up master-to-master replication?

**A.** Duplicate indexes can be a problem, when clients make changes to the database on both mastesr at the same time. To mitigate this configure both masters to use auto\_increment\_increment and auto\_increment\_offset values.

[http://img1.blogblog.com/img/icon18_email.gif](http://www.blogger.com/email-post.g?blogID=5599759766217068450&postID=7372229549733031665)

****Q: - What do you mean a File System?****

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

**Q: - Tell me the name of directory structure hierarchy for Linux**

/root  
/boot  
/bin  
/sbin  
/proc  
/mnt  
/usr  
/var  
/lib  
/etc  
/dev  
/opt  
/srv  
/tmp  
/media

**Q: - What does /boot directory contains?**

The /boot/ directory contains static files required to boot the system, such as the Linux kernel, boot loader configuration files. These files are essential for the system to boot properly.

**Q: - Explain /proc filesystem?**

/proc is a virtual filesystem that provides detailed information about Linux kernel, hardware’s and running processes. Files under /proc directory named as Virtual files. Because /proc contains virtual files that’s why it is called virtual file system. These virtual files have unique qualities. Most of them are listed as zero bytes in size. Virtual files such as /proc/interrupts, /proc/meminfo, /proc/mounts, and /proc/partitions provide an up-to-the-moment glimpse of the system's hardware. Others, like the /proc/filesystems file and the /proc/sys/ directory provide system configuration information and interfaces.

**Q: - Can we change files parameters placed under /proc directory?**

Yes  
To change the value of a virtual file, use the echo command and a greater than symbol (>) to redirect the new value to the file. For example, to change the hostname on the fly, type:   
echo www.nextstep4it.com > /proc/sys/kernel/hostname

**Q: - What is the use of sysctl command?**

The /sbin/sysctl command is used to view, set, and automate kernel settings in the /proc/sys/ directory.

**Q: - If some one deletes /boot directory from your server, than what will happen?**

In that case your server will be in unbootable state. Your Server can’t boot without /boot directory because this directory contains all bootable files

**Q: - What does /dev directory contain?**

The /dev directory contains all device files that are attached to system or virtual device files that are provided by the kernel.

**Q: - What is the role of udev daemon?**

The udev demon used to create and remove all these device nodes or files in /dev/ directory.

**Q: - What kind of files or nodes /dev/ directory contains and how do I access or see device files?**

**Block Device Files:-**

Block device files talks to devices block by block [1 block at a time (1 block = 512 bytes to 32KB)].  
Examples: - USB disk, CDROM, Hard Disk  
  
# ls /dev/sd\*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| brw-rw---- | 1 root | root | 8, | 0 Mar 15 2009 sda |
| brw-rw---- | 1 root | root | 8, | 1 Mar 15 2009 sda1 |
| brw-rw---- | 1 root | root | 8, | 2 Mar 15 2009 sda2 |
| brw-rw---- | 1 root | root | 8, | 3 Mar 15 2009 sda3 |
| brw-rw---- | 1 root | root | 8, | 4 Mar 15 2009 sda4 |
| brw-rw---- | 1 root | root | 8, | 16 Mar 15 2009 sdb |

**Character Device Files:-**   
  
Character device files talk to devices character by character.  
Examples: - Virtual terminals, terminals, serial modems, random numbers  
  
**#ls /dev/tty\***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| crw-rw---- | 1 root | root | 4, | 64 Mar 15 2009 ttyS0 |
| crw-rw---- | 1 root | root | 4, | 65 Mar 15 2009 ttyS1 |
| crw-rw---- | 1 root | root | 4, | 66 Mar 15 2009 ttyS2 |
| crw-rw---- | 1 root | root | 4, | 67 Mar 15 2009 ttyS3 |

**Q: - Tell me the name of device file for PS/2 mouse connection.**

/dev/psaux

**Q: - Tell me the name of device file for parallel port (Printers).**

/dev/lp0