26 Linux Interview Questions and Answers (Basic and Scenarios)

As the opportunities for linux jobs are increasing day by day, it's very adequate to start preparing for Linux interviews. In this article we have presented, questions and answers in basic level and scenarios. More likely all questions are related to system administration.

Basic Questions

1. What is initrd image and what is its function in the linux booting process?

The initial RAM disk (initrd) is an initial root file system that is mounted prior to when the real root file system is available.The initrd is bound to the kernel and loaded as part of the kernel boot procedure. The kernel then mounts this initrd as part of the two-stage boot process to load the modules to make the real file systems available and get at the real root file system. Thus initrd image plays a vital role in linux booting process (https://linoxide.com/booting/boot-process-of-linux-in-detail/).

2. Explain the terms suid, sgid and sticky bit?

In addition to the basic file permissions in Linux, there are few special permissions that are available for executable files and directories.

SUID : If setuid bit is set, when the file is executed by a user, the process will have the same rights as the owner of the file being executed.

SGID : Same as above, but inherits group privileges of the file on execution, not user privileges. Similar way when you create a file within the directory, it will inherit the group ownership of the directories.

Sticky bit : Sticky bit was used on executables in linux so that they would remain in the memory more time after the initial execution, hoping they would be needed in the near future. But mainly it is on folders, to imply that a file or folder created inside a stickybit enabled folder could only be deleted by the owner. A very good implementation of sticky bit is /tmp , where every user has write permission but only users who own a file can delete them.

3. List out few of the differences between Softlink and Hardlink?

a) Hardlink cannot be created for directories. Hard link can only be created for a file.

b) Symbolic links or symlinks can link to a directory.

c) Removing the original file that your hard link points to does not remove the hardlink itself; the hardlink still provides the content of the underlying file.

d) If you remove the hard link or the symlink itself, the original file will stay intact.

e) Removing the original file does not remove the attached symbolic link or symlink, but without the original file, the symlink is useless

4. How do you sent a mail attachment via bash console?

"mutt" is an opensource tool for sending emails with attachments from the linux bash command line. We can install "mutt" from the binary rpm or via package manager.

For Ubuntu / Debian based destros.

```
# apt-get install mutt
```

For Redhat / Fedor based destros,

```
# yum install mutt
```

Usage :

```
# mutt -s "Subject of Mail" -a "path of attachment file" "email address of recipient" < "me
ssage text containing body of the message"
```

Eg : mutt -s "Backup Data" -a /home/backup.tar.gz admin@mywebsite.com < /tmp/message.txt

5. 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

6. 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 the 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 command line , this will move the system from current runlevel to runlevl 3. Current level can be listed by typing the command 'who -r'

7. 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 the 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.

8. 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.

9. 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:

```
<Minute> <Hour> <Day_of_the_Month> <Month_of_the_Year> <Day_of_the_Week>
<command/program to execute>
```

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)
```

10. 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 inode entries store metadata about each file, directory or object, but only points to these structures rather than storing the data. Each entry is 128 bytes in size. The metadata contained about each structure can include the following:

Inode number
Access Control List (ACL)
Extended attribute
Direct/indirect disk blocks
Number of blocks
File access, change and modification time
File deletion time
File generation number
File size
File type
Group
Number of links
Owner
Permissions
Status flags

Inode structure of a directory consists of a name to inode mapping of files and directories in that directory.In a directory, You can find the inode number corresponding to the files using the command `ls -i`

```
786727 -rw------- 1 root root 4226530 May 29 13:17 sudo.log
786437 -rw-------. 1 root root 32640 Jun 23 20:11 tallylog
786440 -rw-rw-r--. 1 root utmp 276096 Jul 20 06:45 wtmp
786741 -rw------- 1 root root 9653 Jul 17 09:38 yum.log
```

Similar way, the number of inodes allocated, used and free in a Filesystem can be listed using `df -i` command

```
# df -i /root
Filesystem Inodes IUsed IFree IUse% Mounted on
/dev/mapper/RootVol-lvmroot
524288 80200 444088 16% /
```

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

Usage : # stat <file name>

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
```

11. Why should I use DAS either NAS or SAN

When we talk about storage, there are some solutions which exist but before choosing one solution, we need to know their role:

DAS is a block device from a disk which is physically attached to the host machine (such as /dev/sda or /dev/sda1) . You must place a filesystem upon it before it can be used. There are limitations like the number of servers that can access it. Storage device, or say DAS storage has to be near to the server storage and the resources are dedicated but generally, you are not able to dedicate the hard disks to multiple computers. DAS solution is inexpensive and simple to configure. Technologies to do this include IDE, SCSI, SATA, etc.
NAS authenticates clients and provides shared to other computers and users over a network so it requires a dedicated ip address to be accessible. NAS devices generally run an embedded operating system on simplified hardware and lack peripherals like a monitor or keyboard. Network file systems can be considered safe enough to be used in a concurrent way, the protocol implementation will take care of problems due to concurrent access to the same resource (file), normally by locking the file to a single user/requester. You can set up automatic or manual backups and file copies between the NAS and all other connected devices by using a software program. It is an easy way to provide RAID redundancy to mass amount of users, it allows users permissions, folder privileges, restricted access to documents, etc
SAN has the particularity to be a block level storage solution that NAS doesn’t provide. It is optimized for high volume of block level data transfer. SAN is performed best when used with fiber channel medium (optical fibers, and a fiber channel switch). It provides synchronous replication and it is an architecture to attach remote storage to make it appear as though it is locally attached. There are highly scalable, both from a capacity and performance perspective. If offers a centralized storage management. It is a solution for terabytes of storage and multiple simultaneous access to files e.g. streaming audio/video and it allows virtual environments, cloud computing, etc.

12. If you are allowed to choose 5 commands, what are your choices?

1) rsync command

The rsync command can be used to synchronize two directories or directory trees whether they are on the same computer or on different computers but it can do so much more than that. rsync creates or updates the target directory to be identical to the source directory.

```
rsync -aH sourcedir targetdir
```

The -a option is for archive mode which preserves permissions, ownerships and symbolic (soft) links. The -H is used to preserve hard links. Note that either the source or target directories can be on a remote host.

2) sed command

You might want to select specific lines of a file. sed, short for stream editor, is one way to do this. you want to combine multiple files that all had headers or to do a bulk find and replace a file.
insert a blank line above every line which matches "regex"

```
$ sed '/regex/{x;p;x;}'
```

change "scarlet" or "ruby" or "puce" to "red"

```
$ sed 's/scarlet/red/g;s/ruby/red/g;s/puce/red/g'
```

3) awk command

awk is a programming language which allows easy manipulation of structured data and the generation of formatted reports. It is mostly used for pattern scanning and processing. It searches one or more files to see if they contain lines that match with the specified patterns and then perform associated actions. It is like sed

Print Specific Field

```
$ awk -F':' '{ print $1 }' /etc/group
$ date | awk '{print $2 " " $6}'
```

4) lsof command

lsof is a command line utility which is used to list the information about the files that are opened by various processes. In unix, everything is a file: pipes, sockets, directories, devices, etc. So by using lsof, you can get the information about any opened files.
List processes which opened a specific file

```
# lsof /var/log/syslog
```

lists all open files belonging to processes owned by the user

```
# lsof -u username
```

Kill all process that belongs to a particular user

```
# kill -9 `lsof -t -u username
```

List all network connections

```
# lsof -i
```

List all network files in use by a specific process

```
# lsof -i -a -c ssh
```

List processes which are listening on a particular port

```
# lsof -i :25
```

5) grep command

grep is a command used to search text or searches the given file for lines containing a match to the given strings or words. By default, grep displays the matching lines.

print network connection used by firefox

```
# netstat -pltnu | grep firefox
```

print the line which contains "root" on /etc/passwd file

```
# cat /etc/passwd | grep root
```

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 ?

Linux Scenario Questions

13. What is the difference between name based virtual hosting and IP based virtual hosting? Explain the scenario where name based virtual hosting seems useful?

Virtual hosts are used to host multiple domains on a single apache instance. You can have one virtual host for each IP your server has, or the same IP but different ports, or the same IP, the same port but different host names. The latter are called "name based vhosts".

n IP-based virtual hosting, we can run more than one web site on the same server machine, but each web site has its own IP address while In Name-based virtual hosting, we host multiple websites on the same IP address. But for this to succeed, you have to put more than one DNS record for your IP address in the DNS database.

In the production shared webhosting environment, getting a dedicated IP address for every domains hosted in the server is not feasible in terms of cost. Most of the customers won't be able to afford the cost of having a dedicated IP address. Here is the place where the concepts of Name based virtual hosting find its place.

14. What is network bonding in Linux and where the important configuration files involved? What is the advantage of Network Bonding?

Network Bonding is a Linux kernel feature that allows to aggregate multiple network interfaces into a single virtual link. This is a great way to achieve redundant links, fault tolerance or load balancing networks in production system. If one of the physical NIC is down or unplugged, it will automatically move traffic to the other NIC card. Similar way the bonding will increase the interface throughput to handle the traffic it it is configured in active-active mode.

There are 7 modes starting from 0 to 6 which decides how the bonding configuration behaves.

mode=0 (balance-rr) - Round-robin policy

It the default mode. It transmits packets in sequential order from the first available slave through the last. This mode provides load balancing and fault tolerance.

mode=1 (active-backup)

Active-backup policy: In this mode, only one slave in the bond is active. The other one will become active, only when the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.

mode=2 (balance-xor)

Transmit the traffic based on [(source MAC address XOR'd with destination MAC address) modulo slave count]. This selects the same slave for each destination MAC address. This mode provides load balancing and fault tolerance.

mode=3 (broadcast)

Broadcast policy: transmits everything on all slave interfaces. This mode provides fault tolerance.

mode=4 (802.3ad)

Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.

mode=5 (balance-tlb) - Adaptive transmit load balancing

channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

mode=6 (balance-alb) - Adaptive load balancing

It includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation.

Important Configuration Files involved:

```
/etc/sysconfig/network-scripts/ifcfg-bond0
/etc/modprobe.d/bonding.conf
/etc/sysconfig/network-scripts/ifcfg-eth[0-4]
/proc/net/bonding/bond0
```

15. Explain briefly the procedure for re-installing Grub in Linux ?

1) Download Ubuntu Installation / Live cd

2) Boot from Ubuntu Installation / Live cd - usb, burned cd etc.
3) During boot select "Try Ubuntu" , Don't select install !
4) Mount your Linux root partition

sudo mount /dev/sda6 /mnt (Assuming /dev/sda6 is the Linux root partition)
5) Install / reinstall grub
$ sudo grub-install --root-directory=/mnt/ /dev/sda (where /dev/sda is your primary disk)
Installation finished. No error reported.

6) Reboot your system, remove bootable CD and we should have the boot menu ready when the system starts.

Note : There would be slight difference when using with other distros.

16. Explain the fields in /etc/passwd and /etc/shadow?

The /etc/shadow file stores actual password in encrypted format with some additional properties related to user password.It mainly holds athe account aging parameters. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file Generally, shadow file entry looks as below.

```
steve:$1$XOdE07rn$WA6qFm4W5UIqNfaqE5Uub.:13775:0:99999:7:::
```

Here is the explanation of each field.

User name : Your login name

Password: Your encrypted password.

Last password change : Days since Jan 1, 1970 that password was last changed

Minimum: The minimum number of days required between password changes.

Maximum: The maximum number of days the password is valid.

Warn : The number of days before password is to expire that user is warned that his/her password must be changed

Inactive : The number of days after password expires that account is disabled

Expire : days since Jan 1, 1970 that account is disabled. It indicates an absolute date specifying when the login may no longer be used

The /etc/passwd file stores essential information, which is required during login /etc/passwd is a text file, that contains a list of user account related parameters like user ID, group ID, home directory, shell, etc.

Here is the sample entry from /etc/passwd file

```
steve:x:6902:6902::/home/steve:/bin/bash
```

Username: User's login name.

Password: An x character indicates that encrypted password is stored in /etc/shadow file.

User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root.

Group ID (GID): The primary group ID

User Info: The comment field. It allow you to add extra information about the user.

Home directory: The absolute path to the directory the user will be in when they log in.

Command/shell: The absolute path of a command or shell (/bin/bash).

17. How do you boot your system into the following modes, when you are in some trouble?

a) Rescue mode
b) Single user mode
c) Emergency mode

Rescue mode provides the ability to boot a small Linux environment from an external bootable device like a CD-ROM, or USB drive instead of the system's hard drive.Rescue mode is provided to help you with your system from repairing the file system or fixing certain issues which prevent your normal operations.

In order to get into the rescue mode, change the BIOS settings of the machine to boot from the external media. Once the system started booting using bootable disk, add the keyword rescue as a kernel parameter or else you can give the parameter "linux rescue" in the graphical boot interface.

In single-user mode, the system boots to runlevel 1, but it will have many more additional functionalities compared to switching to runlevel 1 from other levels.

The local file systems can be mounted in this mode, but the network is not activated.

Use the following steps to boot into single-user mode:

1) At the GRUB splash screen during the booting process, press any key to enter the GRUB interactive menu.
2) Select the proper version of kernel that you wish to boot and type "a" to append the line.
3) Go to the end of the line and type "single" as a separate word.
4) Press Enter to exit edit mode and type "b" to boot into single usermode now.

In emergency mode, you are booting into the most minimal environment possible. The root file system is mounted read-only and almost nothing is set up. The main advantage of emergency mode over single-user mode is that the init files are not loaded. If the init is corrupted, you can still mount file systems to recover data that could be lost during a re-installation. To boot into emergency mode, use the same method as described for single-user mode, with one exception, replace the keyword single with the keyword "emergency".

18. In the ps results, few of the processes are having process state as "D". What does it mean? Briefly explain different process states?

To have a dynamic view of a process in Linux, always use the top command. This command provides a real-time view of the Linux system in terms of processes. The eighth column in the output of this command represents the current state of processes. A process state gives a broader indication of whether the process is currently running, stopped, sleeping etc.

A process in Linux can have any of the following four states…

Running – A process is said to be in a running state when either it is actually running/ executing or waiting in the scheduler's queue to get executed (which means that it is ready to run). That is the reason that this state is sometimes also known as 'runnable' and represented by (R).

Waiting or Sleeping – A process is said to be in this state if it is waiting for an event to occur or waiting for some resource-specific operation to complete. So, depending upon these scenarios, a waiting state can be subcategorised into an interruptible (S) or uninterruptible (D) state respectively.

Stopped – A process is said to be in the stopped state when it receives a signal to stop. This usually happens when the process is being debugged. This state is represented by (T).

Zombie – A process is said to be in the zombie state when it has finished execution but is waiting for its parent to retrieve its exit status. This state is represented by (Z).

Apart from these four states, the process is said to be dead after it crosses over the zombie state; ie when the parent retrieves its exit status. 'Dead' is not exactly a state, since a dead process ceases to exist.

19. What is drop cache in Linux and how do you clear it ?

Cache in Linux memory is where the Kernel stores the information it may need later, as memory is incredible faster than disk.

It is great that the Linux Kernel takes care about that.Linux Operating system is very efficient in managing your computer memory, and will automatically free the RAM and drop the cache if some application needs memory.

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. Now we can throw away that script that allocated a ton of memory just to get rid of the cache.

To free pagecache:

```
# echo 1 > /proc/sys/vm/drop_caches
```

To free dentries and inodes:

```
# echo 2 > /proc/sys/vm/drop_caches
```

To free pagecache, dentries and inodes:

```
echo 3 > /proc/sys/vm/drop_caches
```

This is a non-destructive operation in normal scenarios and will only free things that are completely unused. Dirty objects will continue to be in use until written out to disk and are not freeable. However it is always preferred to run "sync" first to flush useful things out to disk.

20. Password based authentication is disabled in your infrastructure. So how do you login to the servers ?

To improve the system security even further, most of the organizations turned to use keybased authentications instead of Password based authentication. We can enforce the key-based authentication by disabling the standard password authentication, which involves a public key private key pair. The public key is added in the server configuration file while private key is kept confidential on the client side.

Below listed is the procedure, to set up keybased authentication.

1) Generating Key Pairs

a) Generate an RSA key pair by typing the following at a shell prompt:

```
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/steve/.ssh/id_rsa):
```

b) Press Enter to confirm the default location (that is, ~/.ssh/id_rsa) for the newly created key.

c) Enter a passphrase, and confirm it by entering it again when prompted to do so.

d) Copy the content of ~/.ssh/id_rsa.pub into the ~/.ssh/authorized_keys on the machine to which you want to connect,
appending it to its end if the file already exists.

e) Change the permissions of the ~/.ssh/authorized_keys file using the following command:

```
$ chmod 600 ~/.ssh/authorized_keys
```

2) Now on your client side, open the remote connection agent like putty and browse your public key and try SSH to the server, you should be able to login without a password now.

```
# ssh server1.myserver.com
The authenticity of host 'server1.myserver.com (192.168.44.2)' can't be established.
RSA key fingerprint is e3:c3:89:37:4b:94:37:d7:0c:d5:6f:9a:38:62:ce:1b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1.myserver.com' (RSA) to the list of known hosts.
Last login: Tue July 13 12:40:34 2014 from server2.myserver.com
```

3) Public key authentication can prevent brute force SSH attacks, but only if all password-based authentication methods are disabled. Once public key authentication has been confirmed to be working, disable regular password authentication by editing /etc/ssh/sshd_config and set the following option to "no".

```
PasswordAuthentication no
```

21. Explain the different Scenarios involved in TCP 3 way handshake?

The TCP three way handshake is the process for establishing a TCP connection.We can explain 3 way handshake with a simple scenario where we assume a client computer is contacting a server to send it some information.

a) The client sends a packet with the SYN bit set and a sequence number of N.
b) The server sends a packet with an ACK number of N+1, the SYN bit set and a sequence number of X.
c) The client sends a packet with an ACK number of X+1 and the connection is established.
d) The client sends the data.

The first three steps in the above process is called the three way handshake.

22. As the disk space utilization was so high in the server, the Administrator has removed few files from the server but still the disk utilization is showing as high. What would be the reason?

In Linux even if we remove a file from the mounted file system, that will still be in use by some application and for this application, it remains available. Its because file descriptor in /proc/ filesystem is held open..So if there are such open descriptors to files already removed, space occupied by them considered as used. You find this difference by checking them using the "df" and "du" commands. While df is to show the file system usage, du is to report the file space usage. du works from files while df works at filesystem level, reporting what the kernel says it has available.

You can find all unlinked but held open files with:

```
# lsof | grep '(deleted)'
```

This will list the filename which is open with the pid in which it is running. We can kill those Pids and which will stop these process and will recover the disk space responsible for this file.

23. What is rDNS and explain its benefits in the Linux Domain Name Systems?

A typical DNS lookup is used to determine which IP address is associated with a hostname, and this is called Forward DNS lookup. A reverse DNS lookup is used for the opposite, to determine which hostname is associated with an IP address. Sometimes reverse DNS lookups are required for diagnostic purposes. Today, reverse DNS lookups are used mainly for security purposes to trace a hacker or spammer. Many modern mailing systems use reverse mapping to provide simple authentication using dual lookup: hostname-to-address and address-to-hostname. The rDNS (reverse DNS) is implemented using a specialized zone record for reverse lookups called PTR record. PTR records always resolve to names, never IP addresses.

24. What is sosreport, how do you generate it while working with your Redhat Support Team in production?

Sosreport is a command-line utility in Redhat based linux destros (RHEL / CentOS) which collects system configuration and diagnostic information of your linux box like running kernel version, loaded modules, and system and service configuration files. This command also runs external programs to collect further information, and stores this output in the resulting archive. Sosreport is required when you have open a case with redhat for technical support. Redhat support Engineers will require sosreport of your server for troubleshooting purpose. To run sosreport, sos package should be installed. Sos package is part of default installation in most of linux. If for any reason this package is no installed , then use below yum command to install it manually:

```
# yum install sos
```

Generate the report

Open the terminal type sosreport command :

```
# sosreport
```

This command will normally complete within a few minutes. Depending on local configuration and the options specified in some cases the command may take longer to finish. Once completed, sosreport will generate a compressed a file under /tmp folder. The file should be provided to Redhat support representative as an attachment to open a support case.

25. What is swappiness in Linux Memory Management and how do we configure that?

The swappiness parameter controls the tendency of the kernel to move processes out of physical memory and onto the swap disk. Because disks are much slower than RAM, this can lead to slower response times for system and applications if processes are too aggressively moved out of memory.

swappiness can have a value of between 0 and 100 swappiness=0 tells the kernel to avoid swapping processes out of physical memory for as long as possible

swappiness=100 tells the kernel to aggressively swap processes out of physical memory and move them to swap cache

The default setting in Redhat/Ubuntu based Linux distros is swappiness=60. Reducing the default value of swappiness will probably improve overall performance for a typical Ubuntu desktop installation.

```
~$ cat /proc/sys/vm/swappiness
60
```

If we have enough RAM, we can turn that down to 10 or 15. The swap file will then only be used when the RAM usage is around 80 or 90 percent.

To change the system swappiness value, open /etc/sysctl.conf as root. Then, change or add this line to the file:

vm.swappiness = 10

Reboot for the change to take effect

You can also change the value while your system is still running

sysctl vm.swappiness=10

We can also clear swap by running swapoff -a and then swapon -a as root instead of rebooting to achieve the same effect.

26. What is git ?

Git is a very popular and efficient open source Version Control System. It tracks content such as files and directories. It stores the file content in BLOBs - binary large objects. The folders are represented as trees. Each tree contains other trees (subfolders) and BLOBs along with a simple text file which consists of the mode, type, name and Secure Hash Algorithm of each blob and subtree entry. During repository transfers, even if there are several files with the same content and different names, the GIT software will transfer the BLOB once and then expand it to the different files.

Wish you good luck !!!!

Have anything to say?

Your email address will not be published. Required fields are marked *

Name *	Email *

All comments are subject to moderation.

What is linoxide based on ? Windows or Linux ? Type your answer into the box

Submit Your Comment