**User Administration**

**1. What the fields of /etc/passwd file?**

Ans:-

deepak:x:512:512:User:/home/deepak:/bin/bash

1st field: username

2nd field: x tells that an encrypted password is stored in /etc/shadow

3rd field: uid

4th field: gid

5th field: Description

6th field: home directory

7th field: default login shell

**2. How to create a user with specifying a primary/Secondary grp?**

Ans:- useradd -u UPGID -G GroupID username

**3. How can you create a user without useradd command**

Solution:

Step 1

Add an entry of user details in /etc/passwd

The field details are as shown below

username:password:UID:GID:Comments:Home\_Directory:Login Shell

# vi /etc/passwd

user:x:501:501:test user:/home/user:/bin/bash

Step 2

You will have to create a group with same name. So add a new entry in /etc/group

# vi /etc/group

user:x:501:

Step 3

Assign a password to the user

# passwd user

Changing password for user user.

New password:

Retype new password:

passwd: all authentication tokens updated successfully.

Now let us try to login with our newly created user

Ans:-

# su - user

-bash-4.1$

**4. What is the default permission on user's home directory?**

Ans-

700

**5. What is the difference between .bash\_profile and .bashrc?**

Ans:-

Every time you login to a Linux (Red Hat) machine .bash\_profile file is executed

but In case you are already logged in and you open a new terminal then .bashrc file is executed

**7. What is the command to create a user with a pre-defined uid, shell and home directory?**

Ans:-

useradd -m -d /path/to/home -s /bin/bash -u 550 deepak

**8. How to change primary group for any user?**

Ans:-

usermod -g groupname username

**9. If I delete a user, does it's home directory gets deleted? If not then what is the command to delete the home directory of user along with the user**

Ans:-

No.

# userdel -r username

**10. Name any 3 files which are automatically created inside any user's home directory when a user is added**

Ans:-

.bashrc

.bash\_profile

.bash\_history

**11. What is the command to view all the currently logged in users?**

Ans:-

w

**12. What is the command to change and view the expiry date for any user?**

Ans:-

Chage

**13. What are the details you get with finger command?**

Ans:-

Login Details

Mail

Home directory

Last login

**14. How can you give a normal user all the root level privileges?**

Ans:-

Add the user to wheel group and uncomment the wheel group line in sudoers file

Give the user all command permission in sudoers

*Method 1*

# visudo

Add an extra line in the last and make this entry

deepak ALL=(ALL) ALL

Using this above line you are telling your Linux box to give full permission for user deepak on all the hosts and all the commands

[deepak@test ~]$ sudo /etc/init.d/network restart

[sudo] password for test:

Shutting down interface eth0: Device state: 3 (disconnected)

[ OK ]

Shutting down loopback interface: [ OK ]

Bringing up loopback interface: [ OK ]

Bringing up interface eth0: Active connection state: activated

Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/1

[ OK ]

*Method 2*

Add the user to wheel group

# usermod -G wheel deepak

Verify the same

# cat /etc/group | grep wheel

wheel:x:10:root,deepak

Now uncomment this line from sudoers file

# visudo

## Allows people in group wheel to run all commands

%wheel ALL=(ALL) ALL

The reason we did this because be default root is a member of wheel group so in case you want to give root level permission to any normal user then add him/her in wheel group.

$ sudo /etc/init.d/vsftpd restart

Shutting down vsftpd: [ OK ]

Starting vsftpd for vsftpd: [ OK ]

**15. Name any 3 groups of which root is a member by default**

Ans:-

root

bin

daemon

sys

adm

disk

wheel

**16. How can you give sudo access to any user without asking him to provide password every time he runs a command?**

Ans:-

Add an extra parameter NOPASSWD in sudoers file while giving the user permission to run root level commands

**17. Why should I use visudo command instead of directly editing the file with vi or any other editor?**

Ans:-

Well the answer is in case you are editing the sudoers file using vi editor and you use any wrong syntax and save and exit the file then it might even become hard for the root user to log back in and edit the file again. As vi editor would not check for any syntax error inside the file.

That is the reason you should always prefer to use visudo because even in case you make any syntax error then visudo will prompt you before making and changes and exiting.

# visudo

Suppose you want to give your user permission to run network and apache server restart permission

# visudo

%test 192.168.0.100=(root) /etc/init.d/network, /etc/init.d/httpd

**18. Default permission of file and Directory?**

Ans:-

Default permission of file is 644 (666 - 022 (umask vaule))

Default permission of directory is 755 (777 -022 (umask vaule))

**19. How to view the User's login and logout details?**

Ans:-

"last " command will show the users login and logout details.

The command refers /var/log/wtmp to obtain the information.

**20. How to check Primary and Secondary Group of One User ?**

Ans:-

"id -a username" will show the user's Primary and Secondary groups.

FYI, One User can be added in 15 no; of Secondary groups, But Only one Primary Group.

bash-3.00# id -a unixrock

uid=100(unixrock) gid=1(other) groups=1(other)

bash-3.00#

**21. How to lock the User Account ?**

Ans:-

# passwd -l UserID

bash-3.00# passwd -s unixrock

unixrock PS

bash-3.00# passwd -l unixrock

passwd: password information changed for unixrock

bash-3.00# passwd -s unixrock

unixrock LK

bash-3.00#

**22. How to unlock the User Account?**

Ans:-

# passwd -u <UserID>

bash-3.00# passwd -s unixrock

unixrock LK

bash-3.00# passwd -u unixrock

passwd: password information changed for unixrock

bash-3.00# passwd -s unixrock

unixrock PS

bash-3.00#

**23.How to make the user account as non-expriry ?**

Ans:-

# passwd -x -1 <userID>

bash-3.00# passwd -s unixrock

unixrock PS 12/11/13 7 91 7

bash-3.00#

bash-3.00# passwd -x -1 unixrock

passwd: password information changed for unixrock

bash-3.00#

bash-3.00# passwd -s unixrock

unixrock PS

bash-3.00#

**24. How do we set force passwd change for User's first login ?**

Ans:-

# passwd -f <UserID>

bash-3.00# passwd -s unixrock

unixrock PS 12/11/13 7 91 7

bash-3.00#

bash-3.00# passwd -f unixrock

passwd: password information changed for unixrock

bash-3.00#

bash-3.00# passwd -s unixrock

unixrock PS 00/00/00 7 91 7

bash-3.00#

**25. How to delete the User ID ?**

Ans:-

# userdel <UserID> or # userdel -r <UserID>

-r option will delete the User's Home directory too.

**Permissions in Linux**

**1.What is the difference between SUID and SGID?**

Set UID – help to run the program as if the owner is running.

SGID – help to the program as if the group owner is running – Additionally when enabled on directories, the group ownership is inherited by child directories.

2. What is Sticky Bit permission?

When sticky bit is enabled of directories, only the owner of the file is allowed to delete the files and rest of the users cant delete though they have write permission on the directory. Example is /tmp.

**3. What is umask?**

Ans:-

In computing, umask is a command that determines the settings of a mask that controls which file permissions are set for files and directories when they are created. It also refers to a function that sets the mask, and to the mask itself, which is formally known as the file mode creation mask.

**4. What is the default umask value for useradd command and where is it defined?**

Ans:-

Default umask value for useradd: 077

/etc/login.defs

**5. Will you be able to cd into a directory with only read permission?**

Ans:-

No, we need execute permission along with read to cd into directory

**6. What is -R argument used for along with chmod command?**

Ans:-

To recursively apply the permission to all the directories including sub directories and files

**7. How can you restrict a normal as well as root user from making any changes as well as deleting any file?**

Ans:-

chattr command

**8. What is the difference between small t and capital T when applying sticky bit permission?**

Ans:-

Before applying Sticky Bit with executable permission

# chmod 775 /statusupdate

# ls -l

drwxrwxr-x. 3 root root 4096 Oct 17 07:07 statusupdate

After Sticky Bit with executable permission

# chmod 1775 /statusupdate

# ls -l drwxrwxr-t. 3 root root 4096 Oct 17 07:07 statusupdate

Now as you see a small (t) since the directory had executable permission

Before applying sticky bit without executable permission

# chmod 774 /statusupdate

# ls -l

drwxrwxr--. 3 root root 4096 Oct 17 07:07 statusupdate

After Sticky Bit without executable permission

# chmod 1774 /statusupdate

# ls -l

drwxrwxr-T. 3 root root 4096 Oct 17 07:07 statusupdate

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

Ans:-

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

Hardlinks will have same inode numbers

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

**10. 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

**11. What is cron job schedule?**

A cron job is a Linux command for scheduling script on your server to complete repetitive tasks automatically. Scripts executed as a cron job are typically used to modify files, databases and manage caching.

Edit the crontab

$ crontab -e

Display crontab

crontab -l

Display the last edit the crontab file

crontab -v

Locaton of crontab logs

/var/log/cron

**LVM**

**1.How many volume groups can be created in Linux ?**

Answer :256.

Is it possible to increase the logical volume on fly ?

Answer: Yes.We can increase the logical volume without umount it.

**2.How to reduce the logical volume ? is it possible to reduce on fly ?**

Answer: No.You can’t reduce the logical volume on fly. Here is the steps to reduce the logical volume on redhat Linux.

Un-mount the filesystem

Run e2fsck on the volume device

Reduce the Filesystem.(resize2fs)

Reduce the logical Volume(lvreduce)

Mount the filesystem back for production.

**3. How to increase the logical volume?**

Lvextend –L +sizeInMBorGB /dev/vg/lv /dev/pv1 /dev/pv2 ….

4**. How to do you scan the new LUN or disk for LVM physical volume?**

Answer:Use “pvscan” to scan existing physical volume from newly connected SAN or DISKS.

**5. How to scan disks for existing volume group ?**

Answer:Use “vgscan” to scan existing volume group from newly connected SAN or DISKS.

But you should use “pvscan” prior to executing this command.

**6. How to scan a logical volume from exising volume group?**

Answer: lvscan

**7. How to stop the logical volume ? or deactivate the logical volume ?**

Answer: “lvchange -an /dev/vg\_name/lv\_name”

8**.How to activated the logical volume which in deactivated state ?**

Answer: “lvchange -ay /dev/vg\_name/lv\_name” .

**9.How to disable the volume group ? or Deactivate the volume group ?**

Answer:”vgchange -an volume\_group\_name” .

**10.How to enable the volume group ? or Activate the volume group ?**

Answer:”vgchange -ay volume\_group\_name” .

**11.How do you find that what are the disks are used for logical volume mirroring ?**

Answer: use “lvs -a -o +devices”

**12. How to list the imported volume groups?**

Answer: Use “vgs” command to display the imported volume group.

**13. How to list the available logical volumes on the system?**

Answer: Use “lvs” command to list the available logical volumes on the system.

**14.How to list the available physical volumes in LVM?**

Answer: Use “pvs” command to list the available physical volumes.

**15.How to see the detailed volume group information ?**

Answer: Use “vgdisplay vg\_name”

**16.How to see the detailed logical volume information ?**

Answer: Use “lvdisplay /dev/vg\_name/lv\_name”

**17.How to see the detailed physical volume information ?**

Answer: Use “pvdisplay /dev/disk\_name” Ex: pvdisplay /dev/sde

**18.How to rename volume Group ? Can we rename the VG on fly ?**

Answer:Yes.Its possible to rename the volume group on fly.But the mounted volumes will not reflect the same unless you re-mount the volume with new VG name.

Need to update the /etc/fstab with new VG name to mount the volumes across the system reboot.

**19.How to take a LVM configuration backup ?**

Answer:Use “vgcfgbackup vg\_name” to take the latest configuration backup of volume group.The default volume group backup location is “/etc/lvm/backup” .

**20.How to re-create the device files for LVM volumes ?**

Answer: Run “vgmknodes” to recreate the LVM devices files.

**21.What is lvmdump ?**

Answer: “lvmdump” is tool for LVM2 to collect the various information for diagnostic purposes. By default, it creates a tarball suitable for submission along with a problem report

**22.How to replace the failed hard disk in LVM ?**

**23.How to create a mirrored logical volume ?**

**24.How to create a striped Logical volume ?**

**25.How to convert the linear volume to mirror volume ?**

**26.How are snapshots in LVM2 different from LVM1 in Redhat Linux?**

Answer:LVM1 snapshots are readonly by default where LVM2 snapshots were read/write.

**27.What are the steps involved to create the logical volume from scratch ?**

Answer:

i.Create a physical volume using pvcreate command.

#pvcreate /dev/sdc

ii.Create a volume group using “vgcreate” command

#vgcreate vg02 /dev/sdc

iii.Create a logical volume using “lvcreate” command

#lvcreate -L 100M -n vol1 vg02

iv.Create a filesystem on logical volume using mkfs command.

#mkfs -t ext4 /dev/vg02/vol1

v.Mount the filesystem using mount command for use.

#mount -t ext4 /dev/vg02/vol1 /vol1

**28.How to extent the volume group ?**

Answer:Using “vgextend” we can increase the volume group.

**29.Assume Volume group “vg02” is already exists.How do you extend the volume group with 50GB ? Provide all the steps with commands.**

Answer:

1.Get the 50GB lun from SAN team.(/dev/sdd)

2.Create physcical volume ( # pvcreate /dev/sdd )

2.Extend the volume group (# vgextend vg02 /dev/sdd)

**30.If the vg02 has two physical volumes called /dev/sdc/ & /dev/sdd. How do you remove /dev/sdd from vg02.**

Answer: “vgreduce vg02 /dev/sdd/”

**31.How to decommission/remove LVM completely from the host ?**

Answer:

1.Un-mount all the logical filesystems

2.Remove the logical volumes using “lvremove” command.

3.Destroy the volume group using “vgremove” command.

4.Use “pvremove” command remove the physical volumes from the system.

**Networking**

**1. How do you perform NIC teaming & its benefits?**

http://www.golinuxhub.com/2014/01/how-to-do-ethernetnic-bondingteaming-in.html

Load balancing

Fault Tolerance

Failover

**2. What is the difference between TCP and UDP protocol?**

TCP is a connection oriented protocol and contain the information of sender as well as receiver.

Eg: HTTP.FTP, Telnet

TCP is slower than UDP due to its error checking mechanism

UDP protocols are connection less packets have no information to where they are going. These Type of ports are generally used for broadcasting.

For eg: DNS, DHCP

UDP are faster

**3. Mention all the network configuration files you would check to configure your ethernet card**

/etc/sysconfig/network-scripts/ifcfg-eth\*

/etc/sysconfig/network

/etc/resolv.conf

/etc/nsswitch.conf

**4. What is the the use of /etc/resolv.conf?**

Ans: It contains the details of nameserver i.e details of your DNS server which helps us connect to Internet

**5. What is the use of /etc/hosts file?**

To map any hostname to its relevant IP

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

Ans:- nmap localhost

7. **What is the command to check all the listening ports and services of your machine?**

Ans:- netstat -ntlp

**8. How can you make a service run automatically after boot?**

Ans:- using chkconfig command

Chkconfig serviceName on

**9. What is a 3 way handshake protocol? Give an example of it**

SYN - system 1 sends SYN signal to rmote system

SYN-ACK - remote sysstem receives the syn signal and sends ack signal

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

For Example: When you ping to a machine you are sending a SYN signal which is ACK by the remote machine then it sends a SYN ACK signal back to the host machine. Then the host machine receives SYN ACK and sends the ACK signal back to confirm the same.

**10. What are the possible ways to check if your system is listening to port 67**

# nmap localhost | grep 67

# netstat -ntlp | grep 67

**Advance level of questions**

1.How will you restrict IP so that the restricted IP’s may not use the FTP Server?

Answer : We can block suspicious IP by integrating tcp\_wrapper. We need to enable the parameter “tcp\_wrapper=YES” in the configuration file at ‘/etc/vsftpd.conf’. And then add the suspicious IP in the ‘host.deny’ file at location ‘/etc/host.deny’.

Block IP Address

Open ‘/etc/hosts.deny’ file.

# vi /etc/hosts.deny

Add the IP address that you want to block at the bottom of the file.

#

# hosts.deny This file contains access rules which are used to

# deny connections to network services that either use

# the tcp\_wrappers library or that have been

# started through a tcp\_wrappers-enabled xinetd.

#

# The rules in this file can also be set up in

# /etc/hosts.allow with a 'deny' option instead.

#

# See 'man 5 hosts\_options' and 'man 5 hosts\_access'

# for information on rule syntax.

# See 'man tcpd' for information on tcp\_wrappers

#

vsftpd:172.16.16.1

2.Tell us the difference between Telnet and SSH?

Answer : Telnet and SSH both are communication protocol which are used to manage remote system. SSH is Secured, which requires exchanging of key opposite of telnet which transmit data in plain text, which means telnet is less secure than SSH.

1.Explain Linux booting process

BIOS 🡪

MBR 🡪Grub 🡪 Kernel 🡪 Init 🡪 Runlevels

Indetail:-

BIOS: Basic Input Output system Executes MBR

MBR : MBR Excutes GRUB

GRUB : Grub Executes Kernel

Kernel: Kernel Executes /sbin/init

Init : Init executes runlevel programs

Runlevel: Runlevel programs are executed from /etc/rc.d/rc\*.d/

2.Define BIOS and MBR

BIOS refers Basic Input Output system, a boot strap code that executes MBR

MBR: MBR, master boot record, a small program what executes when the computer is booting, usually store first 512 bytes bootable disk.

3.Explain GRUB

Ans:- GNU GRUB (or just GRUB) is a boot loader package that supports multiple operating systems on a computer. During boot-up, the user can select the operating system to run

4.How would you define initramfs and what is its function in the Linux booting process?

Ans:- The only purpose of an initramfs is to mount the root filesystem. The initramfs is a complete set of directories that you would find on a normal root filesystem. It is bundled into a single cpio archive and compressed with one of several compression algorithms. At boot time, the boot loader loads the kernel and the initramfs image into memory and starts the kernel. The kernel checks for the presence of the initramfs and, if found, mounts it as / and runs /init

5.What is the difference between rescue and emergency mode?

Rescue mode

Rescue mode is equivalent to single user mode and requires the root password. Rescue mode allows you to repair your system in situations when it is unable to complete a regular booting process. Rescue mode will try to mount all local file systems and start some important system services, but it does not activate network interfaces neither allow multiple users to be logged in.

Emergency mode

Emergency mode provides the most minimal environment possible and allows you to repair your system even in situations when the system is unable to enter rescue mode. In emergency mode, the system mounts the root file system as read-only, does not attempt to mount any other local file systems, does not activate network interfaces.

6.When it is required to boot the Linux box in the rescue mode and how will you boot the server in rescue mode?

7.What is the default port and configuration file for ssh server

8.How will you change default port for ssh server

Change the Port directive in /etc/ssh/sshd\_config file and restart the sshd daemond using service or systemctl command

9.What is the configuration file for ssh client

10.How will you disable root login in linux server

Ans:- in/etc/ssh/sshd\_config file, AllowRoot directive to set No

11.How will you allow only specific users to ssh in your linux server

Use AllowUsers directive in /etc/ssh/sshd\_config file

12.How will you enable debugging option in ssh server?

Start the daemon with sshd –d option.

13.What is the difference between ssh and telnet?

Ssh uses encryption and where as telnet is clear text (hence it is not secure)

14.What is the use of scp command and what is the syntax?

Used to copy files between UNIX servers using encryption/decryption.

Syntax:- scp filestocopy username@remoteserver:/destinatioinDir

15.What is a process? What command is used to list all processes?

Process is a program in running state. Use Ps command to list processes (ex: ps –elf)

16.What is PID and PPID

PID: Process id and PPID is process Parent ID