Bachelor of Science in Information Technology
Linux System Administration
CBCS (NOV-2022) Q.P Code: 53705

Q1 a) Explain the duties of the linux system administrator in creating and managing users. (5)

1. Linux system administrator is a person who has 'root' access that is 'superuser'.It means he has privilege to access everything which includes all user accounts, all system configurations, home directories with all files therein, all file in system.
2. Following are the duties of the linux system administrator:

- Installing and configuring server.
  In the linux world, the word server has a broader meaning than what you might be used to. For instance, the standards Red hat graphical user interface(GUI) requires a graphical layer called XFree86. This is a server. It runs even on a standalone machine with one user accounts. It must be configured.
- Installing and configuring application software.
  It is possible for individual users to install some applications in their home directions drive space set aside for their own files and customizations-these applications may not be available to other users without the intervention of the user who installed the program or the system administrator.
- Creating and maintaining user accounts.
  User can access his own account but administrator has access to every user account. He/she can add, modify, delete or copy user account. He is responsible for maintaining security by providing role on a user account that defines the level of access.
- Backing up and restoring files.
  To minimize the loss of data, administrator must maintain backup of files and he should restore it whenever required. Backing up is only part of story. You need to formulate a disaster recovery plan to bring your system backup in the event of a failure.
- Monitoring and tuning performance.

Monitoring and tuning of performance is essential for linux to work more efficiently. Administrator must identify system bottleneck and should solve them administrator can use system tools to increase performance, he can determine when hardware need to be upgrade.

- Configuring a secure system.
  It is a duty of administrator to involve tasks and decisions to run secure linux system and maintaining data integrity. It provide strong protection to individuals and corporate bodies and protecting parts of system even if it is inder attack.
- Using tools to monitor security.
  Linux is the preferred operating system who demands secure networks, buy it can be easily crack by hackers.It is important for administrator to be aware of tools hackers use and software used to monitor and counter such activity.

Q1b)Write a short on bash **(5)**

- Bash is a command language interpreter. It is widely available on various operating systems and is a default command interpreter on most GNU/Linux systems. The name is an acronym for the 'Bourne Again Shell'.
- To communicate commands to the operating system kernel and the end user issuing these commands. This interface is known as shell. Several shells are available on RHEL. Bash(short for the bourne again shell) is the one that is used in most situations.
- Bash has a several features that make the command line usage easier and more effective you do not have to always type the whole command line character by character when you are trying to command, you can go backwards and forward by using the leftwards and rightwards arrow keys.
- There are 7 types of bash shell as sh or bourne shell, bash or bourne again shells,csh or c shell, tcsh or TENEX c shell, ksh or the kornshell,zsh,sash.
- Basically, from the bash environment, an administrator is working with commands. An example of such a command is ls, which can be used to display a list of files in a given directory.

- Some shells offer the option to complete a command automatically. It can also complete filenames and shell variables. To use this nice features of completion,use the Tab key.
- For example, the cat command is used to display the contents of an ASCII text file. The name of this file, which is in the current directory, is this_is_a_file. To open this file, the user can type cat thi and then immediately hit the Tab key. If there is just one file that starts with thr letters this, Bash will complete the name of the current directory there is a file with the name this_is_a_ text_file and thisAlsoAFile. Since both files start with this, Bash completes only up to this and doesn't go any further. To display a list of possibilities, you can then hit the Tab key again. This allows you to enter more information manually. Of course, you can then use the Tab key to use the completion feature again.

Q1c) Discuss the difference between piping and redirection with the help of an example. (5)

- The piping and redirection options are among the most powerful features of the linux command line.Piping is used to send the result of a command to another command, and redirection sends the output of a command to a file.
- The Pipe is a command in Linux that lets you use two or more commands such that output of one command serves as input to the next. In short, the output of a process can be give as input to the next one like a pipeline. The symbol 'I' denotes a pipe.
- Pipes help you mash-up two or more commands at the same time and run them consecutively. You can use powerful commands which can perform complex tasks in a second.

Let us understand this with an example.

- When you use 'cat' command to view a file which spans multiple pages, the
- prompt quickly jumps to the last page of the file, and you do not see the content in the middle.
- To avoid this, you can pipe the output of the 'cat' command to 'less' whichwill show you only one scroll length of content at a time.
  $cat /etc/passwd Scat /etc/passwd

| less | more

- Redirection is a feature in Linux such that when executing a command, you can change the standard input/output devices. The basic workflow of any Linux command is that it takes an input and give an output.
- The standard input (stdin) device is the keyboard. The standard output (stdout) device is the screen.

With redirection, the above standard input/output can be changed.

Output Redirection

- The '>' symbol is used for output (STDOUT) redirection [Megabyte@pclDesktop]$ echo This is Megabytes> filel.txt [Megabyte@pc1 Desktop]$ cat filel.txt This is Megabytes.

- Use the correct file name while redirecting command output to a file there is an existing file with the same name, the redirected command will dele the contents of that file and then it may be overwritten." If you do not want a file to be overwritten but want to add more content to an existing file, then you should use '>>' operator.

Megabytepcl Desktops echs This is megaytes> file3.txt
Megabytepcl Desktop $ cat file3.txt
This is Megabytes
$ echo Welcome to megabytes>>file3.txt
Megabytepe Desktops $ cat file3.txt
This is megabytes
Welcome to megabytes

Input redirection

- The '<' symbol is used for input (STDIN) redirection. Megabyte@pc1 Desktop/s we-1 files.txt

files.txt
Megabytepc1 Desktop1s wel<files.txt

- Example: The mail program in Linux can help you send emails from the Terminal.
- You can type the contents of the email using the standard device

keyboard But if you want to attach a File to email you can use the input re-direction operator in the following format.
mails "Subject" to-address < Filename

- When using redirection, you should be aware that it is possible not only toredirect STDOUT and STDIN. Commands can also produce error output. Thiserror output is technically referred to as STDERR.

- To redirect STDERR, use the 2> construction to indicate that you areinterested only in redirecting error output. This means that you won't seeerrors anymore on your current console, which is very helpful if yourcommand produces error messages as well as normal output.
- One of the interesting features of redirection is that, not only it is possible to redirect to regular files, but you can also redirect output to device files. In many cases, however, this works only if you're at the root.
  Standard input STDIN - 0
  Standard output STDOUT - 1
  Standard error STDERR - 2

Q1d) With the help of an example, write the steps to mount a device in linux . (5)

- As an administrator , we need to make storage devices like USB flash drives, hard drives or network shares available. To do this, we need to connect the device to a directory in the root file system. This process known as mounting the device.
- When working with USB flash drive, it should be formatted in supported file system like FAT orExt4 when USB is connected to GUI it will create a subdirectory under/media and its content will be available under the subdirectory.
- MOUNTING USB TO SYSTEM STEPS:
  1. Open a terminal and type su followed by root's password to gain root privilege.
  2. Insert a USB flash drive in the USB port of your computer.(USB should have fat format file system format usin g windows computer).

3. Type of command to find the device name and partition with the name of /dev/sdb1.
4. Create a mount point. #mkdir/mnt/test.
5. Use #mount –t vfat/dev/sdb1/mnt/test to mount the USB flash drive on the /mnt/test directory.
6. Use #cel/mnt/test to go into the /mnt/test directory.

Q1e) List the differencesbetween Hard and Symbolic link. (5)

HARDLINK:

- If the original file is deleted, the file data can still be accessed through other hardlinks.
- If the original file is moved, hard links still work.
- A hardlink can only refer to a file on the same file system.
- The inode and file data are permanently deleted when the number of hard links is zero.
- A hardlink works by creating another filename that refers to the inode data of the original file. This is similar to creating a copy of the file.
- A hardlink preserves the contents of the file.
- A hardlink cannot be created for directories, and they cannot cross filesystem boundaries or span across partitions.
- In hardlink, you can use any of the hardlink names created to execute a program or script in same manner as the original name given.
- A hardlink is a directory entry that associates a name with a file.

SOFTLINK:

- If the symbolic link file is deleted, the original data remains.
- If the original file is moved or deleted, the symbolic link won't work.
- A softlink can refer to a file on a different file system.
- Softlink are often used to quickly access a frequently used file without typing the whole location.
- A softlink points to another entry somewhere in the file system.
- A softlink has the ability to link to directories, or to files on remote computers networked through NFS.

- Deleting a target file for a symbolic link makes that link useless.
- Softlink is a term for any file or directory in the form of an absolute or relative path and that affects pathname resolution.

Q1f) Explain the steps to create and manage your own repository in yum. **(5)**

- STEP 1:
  'Install createrepo utility.'

To create a yum repository we need to install additional software called 'createrepo'
sudo yum install createrepo

- STEP 2:
  'Create a repository directory.'

you need to create a new directory that will be the location of your yum repository and will hold the desired rpm package files. So you should decide the location of this directory and create it.
mkdir<your_directory_name>
as an example let's use /opt/rpms
mkdir /opt/rpms

- STEP 3:
  'Put RPM files into the repository directory.'

You should just copy or download your RPMs into the new directory

- STEP 4:
  'Create the repository metadata.'

The createrepo command reads through the directory with rpm packages and creates a new directory called "repodata" in it. This directory contains the metadata information for the repository. Every time you add additional rpm package files to your yum repository, you need to re-create the repository metadata with the "createrepo" command. So to create the repository you need to execute:
createrepo<path_to_your_directory_with_rpms>
example:
createrepo /opt/rpms
If you already created the repository metadata and you are just adding

new packages to it you need to update the repo:
createrepo --update /opt/rpms

- STEP 5:
  'Create the repository configuration file.'

A yum repository has its own configuration file and there are a few rules for it:It must be located in /etc/yum.repos.d/ directory.
It must have the .repo extension, to be recognized by yum
File options are:

- Repository ID – One word unique repository ID (example: [myrepo])
- Name – Human-readable name of the repository (example: name=My Repository)
- Baseurl – URL to the repodata directory. You can use file://path if repository is located locally or ftp://link, http://link, https://link if repository is located remotely – HTTP Authentication available http://user:password@www.
- Enabled – Enable repository when performing updates and installs (example: enabled=1)
- Gpgcheck – Enable/disable GPG signature checking (example: gpgcheck=1)
- Gpgkey – URL to the GPG key (example: gpgkey=http://mirror.cisp.com/)
- Exclude – List of the packages to exclude (example: exclude=httpd,mod_ssl)
- Includepkgs – List of the packages to include (example: include=kernel)

Required yum repository configuration file options are:

- Repository ID
- Name
- Baseurl
- Enabled
- For example:
- INI
- [customrepo]
- name=CustomRepository
- baseurl=file:///opt/rpms

- enabled=1
- gpgcheck=0

Q2a)Explain the different kinds of partitions in linux and their characteristics. (5)

- There are three types of partitions in linux:
  - Primary partitions
  - Extended partition
  - Logical partition
- Primary partition:

  This information is written in MBR. Maximum of four partitions can be created even if disk space available. There's space for just four partitions in the partition table and no more than four.Each hard disk must have at least one primary partition where you can create a logical volume. You can set only one partition as an active partition. Primary partitions are assigned drive letters.

- Extended Partition: This type can be used if we want to use more than four partitions. A primary partition can have one extended partition.When you want to have more partitions on a basic disk, you can create an extended partition to meet your extra disk partition requirements. You can create logical drives in the extended partition to organize your data files.

- Logical Partitions: A logical partition (not to be confused with a logical volume) is created inside an extended partition. You can have a maximum of 11 logical partitions per disk, and you can create file systems on top of logical partitions.You use logical drives to organize your data files when there aren't enough primary partitions to meet your storage requirements. Unlike primary and extended partitions, logical drives are not assigned any drive letters. You can create any number of logical drives within the extended partitions.

Q2b) Discuss the steps to create a swap file. **(5)**

- Swap space in Linux is used when the amount of physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space.While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM.
- Swap space is located on hard drives, which have a slower access time than physical memory.Swap space can be a dedicated swap partition (recommended), a swap file, or a combination of swap partitions and swap files.
- Use dd to create a file that is filled with all zeroes, which you can use as a swap file:

STEP 1:

Use dd if=/dev/zero of=/swapfile bs=1M count=1024. This command creates a 1GB swap file in the root directory of your server.

STEP 2:

Use mkswap /swapfile to mark this file as swap space.

STEP 3:

Type free -m to verify the current amount of swap space on your server.This amount is expressed in megabytes(MB).

STEP 4:

Type swapon /swapfile to activate the swap file.

STEP 5:

Type free -m again to verify that you just added 1GB of swap space.

STEP 6:

Open /etc/fstab with an editor, and put in the following line:

/swapfile swap swap defaults 0 0

Q2c)What are runlevels in linux?Explain the command used to manage services. (5)

- A run level is a state of init and the whole system defines what system services are operating.The default runlevel to which the system is configured to boot will, in tumdictate which services are started:
- Runlevel 0: The halt runlevel. This is the runlevel at which the system shuts down. For obvious reasons it is unlikely you would want this as
- Runlevel 1: Causes the system to start up in a single user mode under your default runlevel. which only the root user can log in. In this mode the system does not start any networking, X windowing or multi-user services. This run level ideal for system administrators to perform system maintenance or repair activities.
- Runlevel 2: Boots the system into a multi-user mode with text based console login capability. This runlevel does not, however, start the network.
- Runlevel 3: Similar to runlevel 2 except that networking services are started. This is the most common runlevel for server based systems that do not require any kind of graphical desktop environment.
- Runlevel 4: Undefined runlevel. This runlevel can be configured provide a custom boot state.
- Runlevel 5: Boots the system into a networked, multi-user state with XtoWindow System capability. By default the graphical desktop environment will start at the end of the boot process. This is the most common run level for desktop or workstation use.
- Runlevel 6: Reboots the system. Another runlevel that, for obvious reasons, you are unlikely to want as your default

To manage service scripts, following two commands can be used:

1. service command:

Syntax:

#service service_name start/stop/restart status | some more option. This command can manage scripts in the /etc/init.d directory.

2. chkconfig command:
   Syntax:

#chkconfig service_name on | off | list

This command is use to enable, disable, or check Status in the runlevel.

Q2d)Discuss the steps to configure key based SSH authentication. (5)

- The default authentication method in SSH is password based, which means when connecting to a server, you need to enter the password of the user with whom you are connecting.There are two reasons why this might not be ideal. There is a risk that someone can guess your password.
- If you frequently need to connect to the same server, it's a waste of time to enter the identical password over and over.There is an alternative, however; we can use key-based authentication. When SSH key-based authentication is used, you have to make sure the public key is available on the servers to all users who need to use this technology where they want to log in.
- When logging in, the user creates an authentication request that is signed with their private key. This authentication request is matched to the public key of the same user on the server where that user wants to authenticate.
- Before starting create a user in both Linux System. For example, Megabyte. Open terminal and type ssh server-ip-address, Enter current user password Just to check the connection..

  #ssh 192.168.1.6
- Generate public and private key on the client machine using ssh-key #ssh-key. Press Enter to select default file location. Do not enter any paraphrase. Press Enter key twice. This will generate public and private key.
- Transfer your public key to the server. Use ssh-copy-id server-ip-address. #ssh-copy-id 192.168.1.6. To check key based authentication. Login again using ssh server-ip-address.

#ssh 192.168.1.6

This time it doesn't ask any password.

Q2e) Elaborate what basic permissions are and how they are applied to files and directories in linux. (5)

- Every file in Unix has the following attributes:
  Owner permissions: The owner's permissions determine what actions t owner of the file can perform on the file.
  Group permissions: The group's permissions determine what actions user, who is a member of the group that a file belongs to, can perform on the file.
  Other (world) permissions: The permissions for others indicate what action all other users can perform on the file.
- File Access Modes-The basic of permissions are the read, write, and execute permissionswhich have been described below
  Read: Grants the capability to read, i.e., view the contents of the file.
  Write: Grants the capability to modify or remove content of the file.
  Execute: User with execute permissions can run a file as a program.
- Directory Access Modes-Directory access modes are listed and organized in the same manner as anyother file. There are a few differences that need to be mentioned.
  Read: Access to a directory mea
  ns that the user can read the contents. The user can look at the filenames inside the directory.
  Write: Access means that the user can add or delete files from the directory.
  Execute: Executing a directory doesn't really make sense, so think of this as a traverse permission.
- Applying Read, Write, and Execute Permissions
  To change the file or the directory permissions, you use the chmod (changemode) command.
- The three users are represented using a single character:

Character	User
u	User or owner
gGroup user	
o	Other users

aAll three(user, group and other)

- Permission can also be represented using numeric value

Numeric value	Permission
4	Read
2	Write
1	Execute

- Permission format for users:
  d - directory
  r,w,x - Owner permission
  r,wx - Group permission
  r,w,x - Other user permission
- -rwxr--r--: means that owner has read, write and execute permission; group user has only read permission; other users have only read permission. Assign execute permission to all users on file fl

#chmod a+xfl

- Remove execute permission from other users on file fl
  #chmod o-x fl. Assign read and write permission to owner and other user.#chmod uo+rwf1
- Assign read, write and execute permission to user; read and write permission to group user, execute permission to other user.
  #chmod u+rwx,g+rw,0+x f1
- Assign read and write permission to all users
  (rwx:110-6) to all users #chmod 666 fl
- Assign read, write and execute permission to user, read and write permission to group user, execute permission to other user. Userrwx:111-7); groupirs:110-6); other(--x:001-1) #chmod 761 fl

Q2f) Explain the user information configuration file. (5)

- These commands also put all user-related information in some configurationfiles. A configuration file is also used for default settings that are appliedwhenmanaging the user environment.
- /etc/passwd file.This is the most important, of all user-related configuration file. This file is the primary database where user information is stored.
- Different fields are used in /etc/passwd. The fields are separated with a colon.username:password:uid:gid:gecos:home:shell

Fields	Description
Username	The user's account name on the system.
password	username's encrypted password or an x.
uid	username's numeric UID (user ID)
gid	username's numeric primary group ID (group ID)
gecos	An optional field used for informational purpose
home	username's home directory
shell	username's login shell

- Only a root user can modify this file. Use vipw/etc/passwd to avoid locking issues If an error is made, the consequences can be serious. It can evenprevent logging in on a system.To check for error use pwck command without any option.
- /etc/shadow. The encrypted user passwords are stored in /etc/shadow Information relating to password expiry is also kept in this file

- Description of fields in /etc/shadow:
  1.Login name
  2. Encrypted password
  3. Days since January 1, 1970 that password was last changed
  4. Days before password may be changed
  5. Days after which password must be changed warned
  6. Days before password is to expire that user is
  7. Days after password expires that account is disabled
  8. Days since January 1, 1970, that account is disabled
  9. Reserve field, not currently used
- /etc/login.defs is a configuration file that relates to the user environment butis used completely in the background. Some generic settings are defined inthis configuration file.These settings determine all kinds of information relating to the creation ofusers.

Q3 a) State the steps to setup a firewall that allows SSH packets. (5)

- Step 1: Secure your firewall

  If an attacker is able to gain administrative access to your firewall it is "game over" for your network security. Therefore, securing your firewall is the first and most important step of this process. Never put a firewall into production that is not properly secured by at least the following configuration actions:

- Step 2: Architect your firewall zones and IP addresses

  In order to protect the valuable assets on your network, you should first identify what the assets are (for example, payment card data or patient data). Then plan out your network structure so that these assets can be grouped together and placed into networks (or zones) based on similar sensitivity level and function.

- Step 3: Configure access control lists

  Now that you have established your network zones and assigned them to interfaces, you should determine exactly which traffic

needs to be able to flow into and out of each zone.

- Step 4: Configure your other firewall services and logging

  If your firewall is also capable of acting as a dynamic host configuration protocol (DHCP) server, network time protocol (NTP) server, intrusion prevention system (IPS), etc., then go ahead and configure the services you wish to use. Disable all the extra services that you don't intend to use

- Step 5: Test your firewall configuration

  In a test environment, verify that your firewall works as intended. Don't forget to verify that your firewall is blocking traffic that should be blocked according to your ACL configurations. Testing your firewall should include both vulnerability scanning and penetration testing.

Q3 b) What are modules in a firewall?Explain the limit module. (5)

- Use the Firewall module to control access to network resources, network services, and to the Internet by specified applications. A database of known, legitimate applications can automatically be granted access to these resources and services.
- The Firewall module can also protect against port scans, restrict Internet Connection Sharing (ICS), and warn when new nodes join a WiFi connection.
- You should not enable this module if the device is using the Windows built-in firewall, or if the device stays behind a hardware-based firewall.
- Limitations:

➢ Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
➢ Firewalls cannot protect against the transfer of virus-infected files or software.
➢ Firewalls cannot prevent misuse of passwords.
➢ Firewalls cannot protect if security rules are misconfigured.
➢ Firewalls cannot protect against non-technical security risks, such as social engineering.
➢ Firewalls cannot stop or prevent attackers with modems from dialing

in to or out of the internal network.

- Firewalls cannot secure the system which is already infected.

Q3 c) Explainhow to create and manage certificate with openssl. (5)

- Using openssl command-line utility one can create and manage certificates.
  Creating a Self-Signed Certificate :To create sel-signed certificate one need four sub-directories to store the
  certificates: certs, newcerts, private, and crl.
- These subdirectories have already been created on Red Hat Enterprise Linux. Here is an overview of how each of these directories is used:
  1.certs: The storage place for storing all signed PKI certificates. Its open for
  all public as it contains only public keys and no private keys.
  2. newcerts: The temporary storage place for keeping new certificates until they have been signed. Once signed then these can be removed from here.
  3. private: The storage place for storing private keys. This directory needs to be protected as private keys stored over here are the only identity for one's server because once the private keys are manipulated then anyone can access one's server. Keep the mode of directory as 700 to ensure the protection of the directory as only root can access this directory.
  4.crl(certificate revocation list): This list contains certificates that are invalid. And to revoke them in future one needs to copy the the certificates to this directory.
- How to create your own Certificate Authority.
  1.To create a certificate use the configuration file: /etc/pki/openssl.cnf. This file contains default settings that are used to facilitate the creation of new certificates. If certificates are to be placed somewhere else then one need to change the HOME and dir variables from here to reflect the directories used for storing certificates.
  2. Once done with the default values to be used in openssl.conf, one can start creating own self-signed certificate. The following command creates a certificate which uses a 1024-bit RSA key with a

validity of 1 year: #openssl req -newkey md5:1024 -x509 -days 365.

Q3 d) List the steps to encrypt,share and decrypt files using GPG. (5)

- Note that GPG keys are always owned by a user account and not by your entire system. To see the keys that are currently available, use gpg --list-keys
  gpg --list-keys. When using the gpg --list-keys command, one can see only public keys assigned to account. If one wants to check other's private key, use gpg --list- secret-keys instead.

➢ ENCRYPTING FILES WITH GPG

- GPG is commonly used to encrypt files. The base command to do this is easy:
  pg -e yourfile. The gpg command will next ask for a user ID. This is the ID of he user to which you want to send the encrypted file.Using GPG to encrypt a filegpg -e hosts
- The receiver of the encrypted file can decrypt it by using the command gpg - To send it to a new file, make sure to use redirection when specifying the target. The following command: “gpg-d myfile.gpg>myfile”will extract the contents of the GPG encrypted file to myfile.

➢ SHARING FILES WITH GPG

- Signing GPG means data has been transmitted to the intended sender which user's private key is used. This process adds a digital signature tomessage or file. If the receiver of the message has the public key of the sender in their GPG ring, this can automatically prove that the message actually comes from the intended sender.
- The procedure of signing is frequently used in email communications, butcan also be used to sign RPM files. To sign a file, the basic command is gpg -s file. This command can also becombined with -e to encrypt the file. Une gpg-e-s file if you want to encrypt and sign a file at the same time. To open the received signed file use gpg -d to open it.

➢ SIGNING RPM FILES

- When signing RPM packages, the creator of the RPM package needs to through a signing procedure.It results in a signature that can be offered with the RPM package.
- This signature can then be checked against the GPG key, which should be publicly available and imported by the person who wants

to install the

- package.If the signature matches this publicly available GPG key, the person whodownloads the package indeed is guaranteed that the package is signed bythe GPG key, which is joined with the package.

Q3 e) With the help of an example, explain exporting and mounting of NFS share. (5)

- Expoerting, Setting up an NFS server consists of two tasks:
  1.Create the configuration file /etc/exports, which contain the shares you wa to offer.
  2. Start and enable the NFS service.
  3. The following line of code provides an example of a share that you can use /etc/exports:/data 192.168.1.007/24 (rw,no_root_squash)
  4. The line consists of three parts. First, there is the name of the directory
  want to share, or /data in this example.
  5. Next, we specify to whom we want to offer access. In this example, access is offered to the network 192.168.1.007/24.
  6. The access restriction is always host-based, and many options are available to specify which hosts we want to give access.
  7. After putting all of the shares in /etc/exports, we just need to (rejstart the NFS server to activate them and to do this, use #service nfs restart. After a successful start of the NFS server, we can use #showmount -e localhost to check that the shares are available.
- MOUNTING AN NFS SHARE
- Once NFS share is created, it can be accessed from a client machine and for
  this we need to just mount it as if it were a regular file system. The following command is used to mount the NFS share just created:
  #mount mynfsserver:/data /mnt
- For temporary purpose /mnt directory can be used but if one want to mount NFS shares in a more persistent way, it makes sense to create adedicated directory for this purpose.
- Before mounting an NFS share,one can look for shares offered by that server and for this, again use the showmount command with the -e option. This command shows all of the NFS shares offered by the

server in question:
#showmount -e mynfsserver.

Q3 f)Discuss the steps to setup a samba server. (5)

- Samba is a very versatile service that can be used for different purposes on
  your network. Apart from sharing files, it can share printers and also offer Windows domain services such as directory services. The most popular use of Samba is as a file server.
- Setting Up a Samba File Server
  To set up Samba file server, following steps have to be taken care of:
  1. Create a directory on the Linux file system on the Samba server.
  2. If needed, create Linux users and give the appropriate permissions to the directory you just created.
  3. Install the Samba server.
  4. Define the share in /etc/samba/smb.conf.
  5. Create a Samba user account that has access to the share.
  6. (Re)start the Samba service.
  7. Tell SELinux to give access to the Samba share.
- Samba share can be defined by putting it in Samba's main configuration file, which is /etc/samba/smb.conf. The basic share definition consists of a name given to the share, and it tells Samba what to share. A minimum share definition might appear as follows:
  [myshare]
  path=/mysharedfolder
- When defining a share, one can also use many options to define to whom and with which access permissions the share should be available. It could, for example, appear as follows:
  (myshare)
  path-/mydatafiles
  comment some shared files
  allow hosts 192.168.3.
  writable- yes
  public - yes
  write list +mygroup
  In this example share, some options are added.

- First a comment is specified, which makes it easier for clients to identify the
  share when they are browsing the network for available services. Next allow hosts parameter restricts access to hosts that have a starting with 192.168.3 only. The option public yes makes it a public share that is accessible by anyos an IP addreswho has a Samba account to authenticate to this server.
- It is also writable, which is indicated by the option writable - yes.To write to the share, though, a user must be a member of the local Lin group mygroup. When working with Samba, you can use different security options. This option is set in the global section of the /etc/samba/smb.conf file, and determines where Samba looks for user authentication information.
- The default setting is security user, which means that Samba needs a local Samba useaccount that is stored in a smbpasswd file.
- The following authentication options are available:

➢ Security=share:When using this option, a user does not need to sendusername and password to a share before connecting to it. One can set it up that a user has to enter a password before connecting. However, this would be share-level password that is used by every user connecting to the share. Using can be beneficial on an anonymous share, to where you want users to connect with limited permissions. When using this option, use the guest only parameter in the share. Never use it for shares that contain valuable data.

➢ security = user: This is the default security option, where a user must log
  to the share before getting access.

➢ security = domain:This option works if your Samba server has been added
  to a Windows domain.

➢ security = server:This option uses an external server (such as anothe Samba server) to handle Samba authentication requests.

➢ Security=ads: This option makes Samba a member in a Windows Active
  Directory domain. It does not make it a domain controller but integrates Sambain the AD domain, which makes it easier to access resources in the AD domain orto set up access for AD users to

resources in Samba.

- Accessing Samba Shares- To access Samba Server from Windows, one can set up a network share and point to the Samba server. To list the Samba shares that are offered by a specie server, one can use smbclient-L
- This shows the names of all shares that are offered, and it also provides an
  option to log in to the Samba server. When using smbclient -L to list shares
  password is not necessary for listing. So if its asking for password then just need to press Enter key.

Q4 a) Write a short note on cache-only nameserver. (5)

- The job of a DNS caching server is to query other servers and cache the response.
- Next time when the same query is given, it will provide the response from the
  cache. The cache will be updated periodically.
- Configuring a cache-only name server isn't difficult. We just need to install the BIND service and make sure that it allows incoming traffic.
- For cache only name servers, it also makes sense to configure a forwarderto
  optimize speed in the DNS traffic in our network.
- A caching server does not provide information to outsidesources; it is used to provide domain information to otherserversandworkstationson thelocalnetwork.
- The caching server remembers the domains that are accessedpreviously. Caching server speeds up searches since thedomaininformationisalready stored inmemory.

Q4 b) Explain the DHCP server configuration. (5)

- The Dynamic Host Configuration Protocol (DHCP) is used to assign IP-related configuration to hosts in our network. DHCP server makes managing a network a lot easier, because it gives the administrator the option to manage IP-related configuration on a

single, central location on the network, instead of on multiple different hosts.

- A DHCP server can be configured to assign more than 80 different parameters to its clients, of which the most commonly used are IP addresses, default gateways, and the IP address of the DNS name servers. When a client comes up, it will send a DHCP request on the network.
- This DHCP request is sent as a broadcast, and the DHCP server that receives the DHCP request will answer and assign an available IP address. Because the DHCP request is sent as a broadcast, we can have just one DHCP server per subnet.
- If multiple DHCP servers are available, there is no way to determine which DHCP server assigns the IP addresses. In such cases, it is common to set up failover DHCP, which means that two DHCP services together are servicing the same subnet, and one DHCP server completely takes over if something goes wrong.
- When configuring a DHCP server, it is a good idea to think about the default lease time. This is the amount of time that the client can use an IP address it has received without contacting the DHCP server again. In most cases, it's a good idea to set the default lease time to a rather short amount of time, which means it doesn't take too long for an IP address to be given back to the DHCP server.
- This makes sense especially in an environment where users connect for a short period of time, because within the max-lease-time (two hours by default), the IP address is claimed and cannot be used by another client. In many cases, it makes sense to set the max-lease-time to a period much shorter than 7,200 seconds.

Q4 c) Discussrole of MUA,MTA and MDA in the email process. (5)

➢ MUA(mail user agent):

- A Mail User Agent (MUA) is a program that, at the very least, allows a user to read and compose email messages. An MUA is often referred to as an email client. Of course, many MUAS help users do more than that, including retrieving messages via the POP or IMAP protocols, setting up mailboxes to store messages, or helping present new messages to a Mail Transfer Agent that will deliver them to their final destination

- It is the responsibility of users to install an MUA, which allows them to work with email on their computer, tablet, or smartphone.It is called an email client (such as Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail or Lotus Notes& Mutt Tool).
- When it is a web interface used for interacting with the incoming mail server, it is called webmail.An MUA is a program that, at a minimum, allows a user to read and compose email messages.

➢ MTA(mail transfer agent):

- A mail transfer agent or mall relay transfers email messages from onecomputer to another. An MTA is responsible for the core tasks involved with delivering of email, including: queuing, throttling, scheduling, connection management, data transfer, processing of deferrals, bounce generation and tracking of delivery status.
- A Mail Transport Agent (MTA) transports email messages between hosts using SMTP. A message may involve several MTAs as it moves to its intended destination.
- The major functions of an MTA are:
  Accepting messages originating from the user agent and forwarding them totheir destination.
  Receiving all messages that are transmitted from other user agents for further transmission.
  Keeping track of each and every activity and analyzing and storing the recipient list to perform future routing functions.
  Sending auto-responses about non-delivery when a message does not reachits intended destination.
- Relaying is a hot item in email delivery. An MTA doesn't relay messages for just anyone, but only for authenticated users or users who are known in some other way. If messages were relayed for everyone, this would likely mean that the MTA was being abused by spammers on the Internet.
- Queuing means that the MTA stores the message in a local directory and will try to deliver it again later. As an administrator, you can flush the queues, which means that you can tell the MTA to send all queued messages now.
- Upon delivery, it sometimes happens that the MTA, which contacted an exterior MTA and delivered the message there, receives it back. This process is referred to as bouncing.

- In general, a message is bounced if it doesn't comply with the rules of the receiving MTA, but it can also be bounced if the destination user simply doesn't exist. It also generate error message if it's not successfully delivered.
- Red Hat Enterprise Linux offers two MTAs, Postfix and Sendmail, email client programs are often not required to act as an MTA. Red Hat Enterprise Linux also includes a special purpose MTA called Fetchmail.

➢ MDA(mail delivery agent):

- The recipient's MTA then delivers the email to the incoming mail server (called the MDA, for Mail Delivery Agent), which stores the email as it waits for the user to accept it. There are two main protocols used for retrieving email on an MDA: POP3 (Post Office Protocol), the older of the two, which is used for retrieving email and, in certain cases, leaving a copy of it on the server; and IMAP (Internet Message Access Protocol), which is used for coordinating the status of emails (read, deleted, moved) across multiple email clients. With IMAP, a copy of every message is saved on the server, so that this synchronization task can be completed.
- MDAs act as mailboxes, which store messages (as much as their volume will allow) until the recipients check the box. It is also called as LDA (Local Delivery Agent).MDA is protected by a user name called a login and by a password.
- Any program that actually handles a message for delivery to the point where it can be read by an email client application can be considered an MDA.
- MDAs do not transport messages between systems nor do they provide a user interface; MDAs distribute and sort messages on the local machine for an email client application to access
- The MDA delivers mail to the recipient's local message store, which by default on Red Hat Enterprise Linux is the directory /var/spool/mail/$USER. In the Postfix mail server, an MDA is included in the form of the local program.
- To get their messages from a remote desktop you need a POP server that allows users to download messages or an IMAP server that allows users to connect to the mail server and read the messages while they're online.

Q4 d) Explain the various parameters for secure internet configuration of Postfix server. **(5)**

- There are a few more steps to take to configure a mail server, which is going to handle messages from the Internet. Most of the additional tasks relate to security. You'll need to make sure your mail server has at least a minimum level of protection against spam and other email abuses. To make a secure Internet configuration, you need to set some additional parameters. All of these will be set in the /etc/postfix/main.cf file.
  # vi /etc/postfix/main.cf
  Myhostname=
  inet_protocols Ipv4

inet interfaces all alias_maps hash:
/etc/aliases
mydestination=
mynetworks =

/etc/postfix/main.cf
The following are the relevant parameters:

- myhostname: This parameter specifies the internet hostname of this maildaemon. The default is to use the fully-qualified domain name.
- mydestination: This parameter specifies which destinations this machine will deliver locally. Use the configuration locally which has been provided bydefault in the server and change the localhost to the domain name.
- mynetworks: This line is a bit riskier. This entry will define authorizeddestinations that mail can be relayed from. If you are thinking to add yoursubnet here, there are partial chances of its success.
- mydomain: This parameter specifies the domain of this host. If not set, thedomain name part of the FQDN is used.
- myorigin: This parameter determines the domain seen by the email recipient when receiving messages. The default is to use the FQDN of this host. This means that if user tyit on server root.example.com sends a message, the recipient will see a message coming in from tyit@root.example.com.To append the domain name only and not

the entire FQDN, use myorigin. $mydomain.

- inet interfaces: This parameter specifies the IP addresses of the mail server to which it binds. By default, it is set to localhost only, which means that your mail server cannot receive messages from the Internet. To enable all inet_interfaces using inet_interfaces all.
- relayhost: This parameter contains the name of a host that is used to relay all messages to. For example, you want the mail server of your ISP to take care of all message delivery.
- To change any of these parameters which is present in /etc/postfix/main.cf you can change the configuration file by hand and restart postfix afterdoing so.
- Alternatively, you can use the postconf command to monitor and set parameters.

Q4 e) State the steps to setup virtual hosts in Apache. (5)

- Virtual Hosts are used to run more than one domain off of a single Ip address. This is especially useful to people who need to run several sites off of one server.
- The sites display different information to the visitors, depending on with which the users accessed the site.
- There is no limit to the number of virtual hosts that can be added to a server. There are two types of Apache virtual host configurations:
  IP-Based Virtual Host
  Name-based Virtual Host. Name-based virtual host is recommended for most scenarios.

Step 1:

Get machine IP address and hostname.

Step 2:

Add hostname in etc/hosts file
#gedit/etc/hosts

Step 3:

Open httpd.conf file
#gedit/etc/httpd/conf/httpd.conf

Step 4:

Add virtual host information
(Alternatively we can put * instead of IP address)

Step 5:

Create a directory under Document root

#mkdir –p/lib/iso/pc1.megabytes.com

Step 6:

Create an index.html file inder pc1.megabytes.com

Step 7:

Restart httpd service

#service httpd restart

Step 8:

Open web browser and type

Create server 2

Step 9:

#mkdir –p /lib/iso/pc2.megabytes.com

Step 10:

#gedit /lib/iso/pc2.megabytes.com/index.html

Step 11:

http://192.168.1.8/pc2.megabytes.com or http://localhost/pc2.megabytes.com

Q4 f) Explain how the directoryIndex, options allow Override and order directions in Apache. (5)

- First, there is the AllowOverride directive. This directive is related to the .htaccess file that an administrator can use to restrict access to a gives directory.
- If AllowOverride is set to none, the contents of any .htaccess file that is found anywhere in a subdirectory of the current directory will beignored.
- If you don't want the owners of subdirectories to restrict access to their directories, you should set AllowOverride to none. If you want to allow users to restrict access to subdirectories, set it to all.
- Another basic way to handle access restrictions is by using the Order directive. With this directive, you'll specify the order in which allow anddeny commands are used.
- The default order is deny and then allow.This means that if a client is excluded by deny, it will be excluded unless it matches allow. If neither is matched, the client gets access. As you see, this is a rather open approach that doesn't put many restrictions on a directory.

- Look at this example:
  order allow, deny
  allow from 10.100
  deny from all
- In this line, the allow rules are read first and give access to any host that has an IP address starting with 10.100.
- However, after reading the deny line that denies access to all, the site wouldbe closed, even for devices that have an IP address starting with 10.100.
- If you want to make sure that everyone is denied with the exception of devices that have an IP address starting with 10.100, you should rewrite the statement as follows:
  order deny, allow
  allow from 10.100
  deny from all

Q5 a) Discuss the various ways in which a shell script can be executed. (5)

Therearethreedifferent waystoexecutescripts:

- Makeitexecutable,andrunitasaprogram.
- Runitasanargumentofthebash command.
- Sourceit.

MakingtheScriptExecutable:

The most common way to run a shell script is by making itexecutable. To do this with the hello script, use the followingcommand:

chmod+xhello

After making the script executable, you can run it just like anyother command. The only limitation is the exact location in thedirectorystructureofyourscript.Ifitisinthesearchpath,youcanrun it by typing any command. If it is not in the search path, youhavetorun itfromtheexactdirectorywhereitislocated.

RunningtheScriptasanArgumentoftheBashCommand:

The second option for running a script is to specify its name as

runningitthisway.

Sourcingthe Script

The third way of running a script is completely different. You cansource the script. By sourcing a script, you don't run it as a subshell.Rather, you include it in the current shell. This can be useful if thescript contains variables that you want to be active in the currentshell.

Therearetwowaystosourceascript.Thesetwolinesshowyouho wtosourceascriptthathasthenamesettings:

.
setting
ssourc
esettin
gs

Itdoesn't reallymatterwhichoneyouusebecausebotharecompl etelyequivalent.

Q5 b) Write a shell script to add ten user, remove their passwords and add them to the group students use. (5)

```
if [ $(id -u) -eq 0 ]; then
        read -p "Enter username : " username
        read -s -p "Enter password : " password
        egrep "^$username" /etc/passwd >/dev/null
        if [ $? -eq 0 ]; then
                echo "$username exists!"
                exit 1
        else
                pass=$(perl -e 'print crypt($ARGV[0], "password")' $password)
                useradd -m -p "$pass" "$username"
                [ $? -eq 0 ]&& echo "User has been added to system!" || echo "Failed to add a user!"
        fi
else
        echo "Only root may add a user to the system."
        exit 2
fi
```

Q5 c)Explain the steps to setup a quorum disk. (5)

- Quorum is an important mechanism in the cluster that helps nodes determines whether they are part of the majority of the cluster. A quorum disk involves two parts. First a shared storage device is needed that can be accessed by all nodes in the cluster and then heuristics testing will be needed which consists of at least one test that a node has to perform successfully before it can connect to the quorum disk.
- If a situation of split brain arises, the nodes will all poll the quorum disk. If they're capable of performing the heuristics test, the node can count an extra vote toward its quorum. If the heuristics test cannot be executed successfully, the node will not have access to the vote offered by the quorum disk, and it will therefore lose quorum and know that it has to be terminated.
- To set up a quorum disk, following steps need to be performed:
  1. Create a partition on the shared disk device.
  2. Use mkqdisk to mark this partition as a quorum disk.
  3. Specify the heuristics to use in the Conga management interface.

- In Conga, open the Configuration → QDisk tab. On this tab, select the option Use A Quorum Disk. Then the device to be used has to be specified. The best way to refer to the device is by using the label that has been created by using 'mkqdisk' to format the quorum disk. Now heuristics need to be specified.
- This is a little test that a node must perform to get access to the vote of the quorum disk Here ping the Path Program field, enter ping -c 1 192.168.1.20. The interval specifies how often the test should be executed. Five seconds is a good value to start with. The score specifies what result this test yields if executed successfully.
- If several different heuristics tests are connected to a quorum disk, work with different scores can be possible.The TKO is the time to knock out, which specifies the tolerance for the quorum test. Set it to 12 seconds, which means that a node can fail the heuristics test no more than two times.
- The last parameter is Minimum Total Score. This is the score that a node can add when it is capable of executing the heuristics properly. Click Apply to save and use these values. After creating the quorum

device, cman tool status command can be used to verify that it works as expected.

- Look at the number of nodes (which is set to 2) and the number of expected nodes (which is set to 3) The reason for this can be found in the quorum device votes, which is set to 1. This means that the quorum device is working, and you're ready to move on to the next step.

Q5 d)Discuss the steps to setup fencing. (5)

- Fencing is what you need to maintain the integrity of the cluster. Hardware fencing means that a hardware device is used to terminate a failing node. Typically, a power switches or integrated management card.
- To set up fencing, two steps are needed. First step is to configure the fence devices, and then associate the fence devices to the nodes in the network. To define the fence device, Fence Devices tab needs to be opened in the Conga management interface.
- After clicking Add, a list of all available fence devices is displayed. A popular fence device type is IPMI LAN. This fence device can send instructions to many integrated management cards. After selecting the fence device, its properties need to be defined.
- These properties are different for each fence device, but they commonly include a username, a password, and an IP address. After entering these parameters, the device to the configuration can be submitted.
- After defining the fence devices, these are needed to connect to nodes. From the top of the Luci management interface, click Nodes, and then select the node to which fence device need to be added.
- Scroll down on the node properties screen, and click the Add Fence Method button. Next, name is to be entered for the fence method to be used and for each method, click Add Fence Instance to add the fence device created here. Submit the configuration, and repeat this procedure for all the nodes in your cluster.

Q5 e) Explain the steps to perform an automated installation using a kickstart file. (5)

- Kickstart file is used to perform a completely automated installation and how it can be optimized as per the needs.Using a Kickstart File to Perform an Automated Installation For using kickstart file to install a server, installer need to be specified the path of the file for it.
- For example, if the kickstart file is copied to the server1.example.com web
  server document root, add the following line as a boot option while installing
  from a DVD:
  linuxks=http://server1.example.com/anaconda-ks.cfg
- To use a kickstart file in an automated installation from a TFTP server, addition of the kickstart file to the section in the TFTP default file that starts the installation is needed. 16.3.2 Modifying the Kickstart File with system-config-kickstart
- In the previous exercise, kickstart installation was started based on the kickstart file created after the installation of server finished. To avoid the questions asked during installation it needs to fine-tune the kickstart configuration file which can be done using system-config-kickstart and new kickstart files can be created.
- The system-config-kickstart interface looks like the one used to install an RHEL server, and all options are offered in different categories, which are organized similar to the screens that pose questions during an installation of Red Hat Enterprise Linux. File → Open option to can be used to read an existing kickstart file.
- Under Boot Loader Options, installation of a new boot loader can be specified and where it has to be installed. If specific kernel parameters are needed while booting, that also can be specified. Kickstarts can be updated about the partitions to be created on the server. By default, the Network Configuration option is empty.
- If networking is needed on the server, Add Network Device option to be used indicating the name of the device and how it can obtain its network configuration.The Authentication option offers tabs to specify external authentication services such as NIS, LDAP, Kerberos, and some others.

- If not specified any of these then default to the local authentication mechanism that goes through /etc/passwd, which is fine for many servers. If server is connected directly to the Internet, turn firewall on and select all of the trusted services that can be allowed. For the Display Configuration option, installer can be informed whether server should install a graphical environment.
- An interesting option is Package Selection. This option allows selecting package categories; however it does not allow selecting individual packages. If individual packages need to be selected, manual configuration is needed.
- Finally, there are the Pre-Installation Script and Post-Installation Script options that allow adding scripts to the installation procedure to execute specific tasks while installing the server.

Q5 f) List the steps to configure DHCP PXE boot. (5)

- PXE Boot allows booting a server need to install from the network card of the server. The PXE server then hands out a boot image, which the desired installation server uses to start the initial phase of the boot.
- Two steps are involved:
  1. Firstly TFTP server needs to be installed and have it provide a boot image to PXE clients.
  2. Second DHCP needs to be configured to talk to the TFTP server to provide the boot image to PXE clients.
- Installing the TFTP Server
  1. To install the TFTP server package using yum y installtftp-server. TFTP is managed by the xinetd service, and /etc/xinetd.d/tftp file needs to be opened to tell xinetd that it should allow access to TFTP and change the disabled parameter from Yes to No.
  2. Next, restart the xinetd service using service xinetd restart. Also make sure to make xinetd on during boot time using chkconfigtftp on.
  3. TFTP server is configured and ready to use now. Next is to configure DHCP to communicate with the TFTP server to hand out a boot image to PXE clients.
- Configuring DHCP for PXE Boot, Modify the DHCP server configuration so that it can hand out a boot image to PXE clients. To do this, include the boot lines in /etc/dhcpd/dhcpd.conf file, and

restart the DHCP server.

- The most important part of the example configuration in the above listing file is the class pxeclientsdefinition.The match line ensures that all servers that are performing a PXE boot are recognized automatically.
- This is done to avoid problems and to have DHCP hand out the PXE boot image only to servers that truly want to do a PXE boot. Next, the next-server statement refers to the IP address of the server that hand out the boot image. This is the server that runs the TFTP server. Finally, a file is handed out.