



RedHat Certified Engineer (RHCE)+(RHCSA)

RHCE certification is one of the most respected IT certification programs worldwide. Red Hat Certified Engineer (RHCE) is earned by a Red Hat Certified System Administrator (RHCSA) who has demonstrated the knowledge, skill and ability required of senior system administrator for Red Hat Enterprise Linux systems.

this system. From RHCE7 installation is not covered in exam. It means you are getting a pre RHEL installed system in exam. RHCE 7 exam cover virtualization of RHEL. For virtualization you still need to know the installation of RHEL.

Minimum hardware requirement for rhel 7

Minimum hardware requirement would be discussed in this article. Before you prepare a server system for exam practice, it is good idea to have a look on minimum hardware requirement for rhel7. This minimum requirement is outlined only for RHCE exam prospective.

64 Bit system

During the exam you need to configure KVM and KVM operate only on 64 bit system. So you need a 64 bit system for exam preparation. For the practice of exam, we need to install RHEL 7. And to configure a system for KVM, which requires hardware assisted virtualization. For this we need a system with 64-bit CPUs and related hardware.

Architectures

For exam prospective you need not worry about architecture as in exam you get a live system with proper architecture. For practice prospective you should use Intel/AMD 64-bit or x86_64 architecture for the RHCSA and RHCE exams.

RAM Requirements

Officially Red Hat requires 512MB of RAM and recommends at least 1GB of RAM per system. Red hat OS is designed in such a way that it could run smoothly even on 200 MB RAM (ON VM without GUI).

Maximum Ram supported by RHEL7 is 16GB on 32-bit systems and 32GB on 64-bit systems.

For practice we suggest you use a system with at least 2 GB RAM 1 GB for host RHEL system and 1 GB for KVM.

Hard Drive

Red hat require minimum 12GB of free space but for the practice we suggest you to use a hard disk with minimum 40 GB free space on server. During the practice we would host another machine in KVM and would make a dump of rhel7 disk on server for network installation. Start practice with minimum 40 GB free disk space.

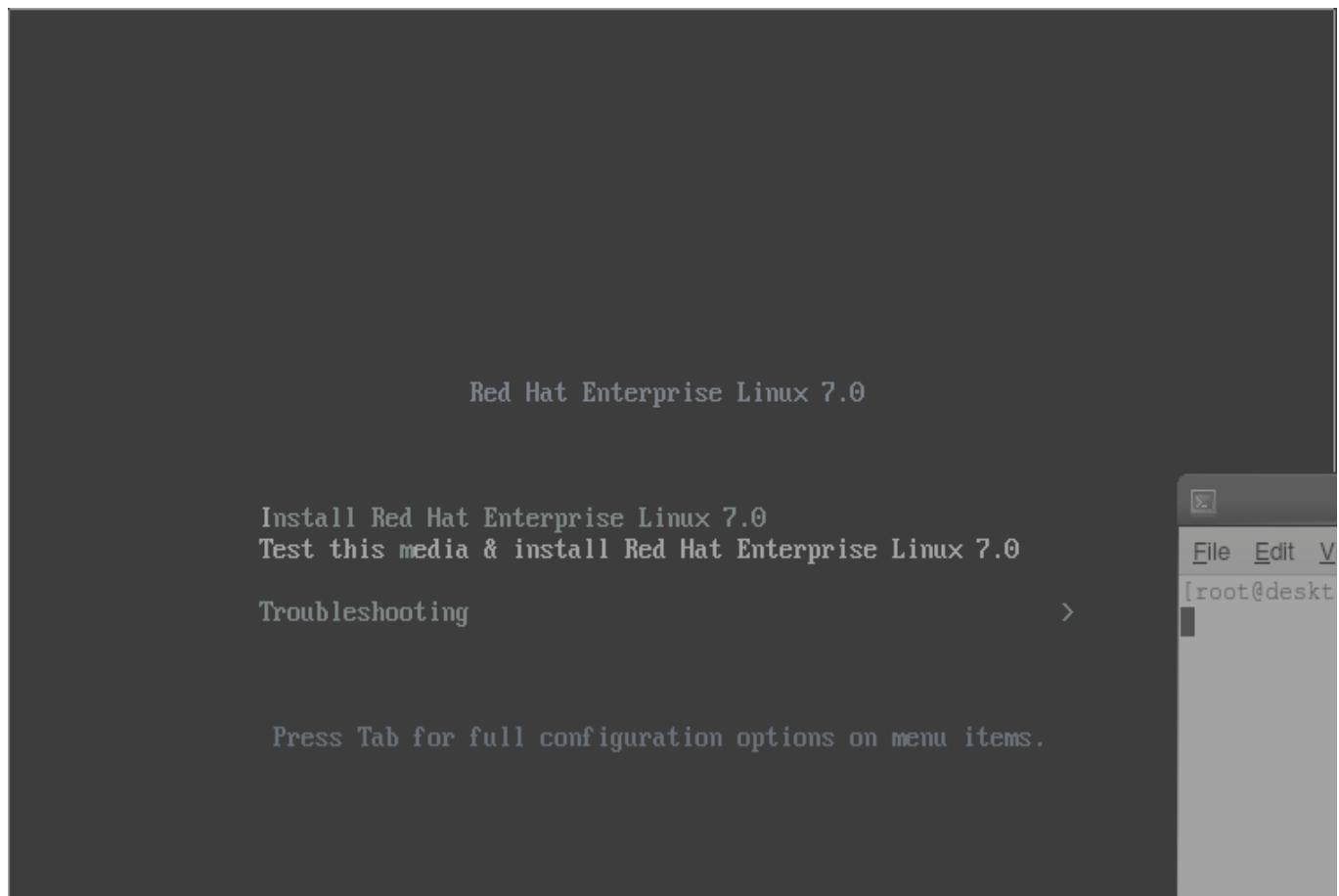
CDROM Drive

Red Hat does not include a floppy version of the boot images in RHEL7. Your system will need a boot-capable CDROM drive, or BIOS capable to boot form PXE.

how to install RHEL7 from dvd

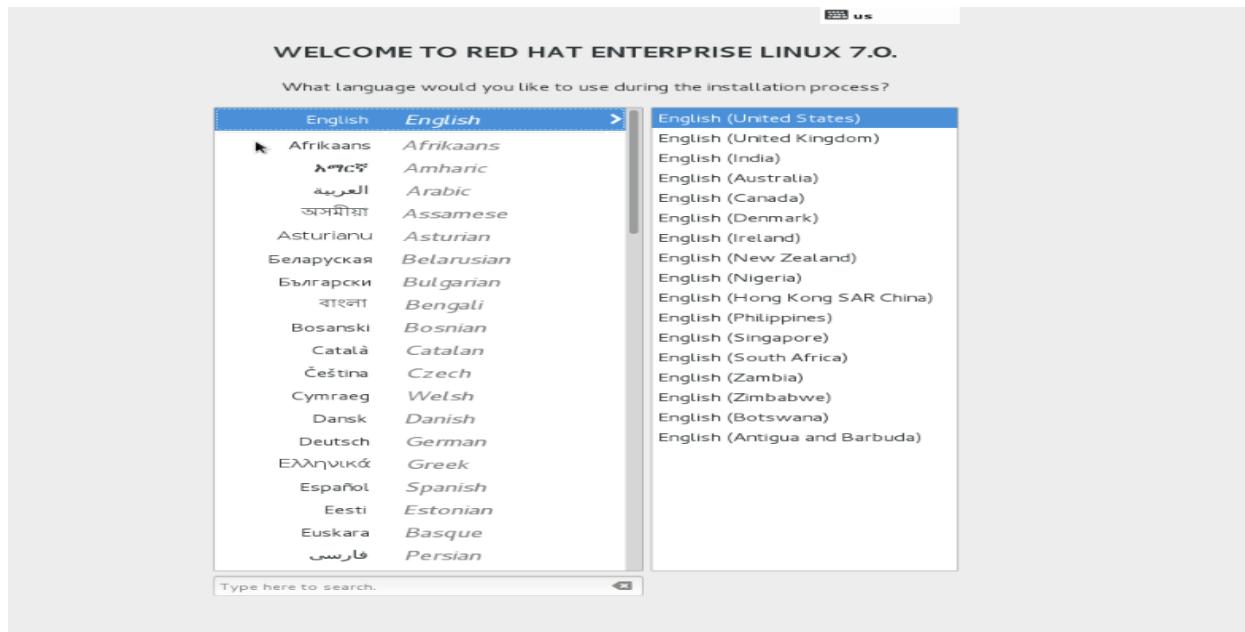
In this article I would show you how to install RHEL7 on physical system from media. We would set up a physical system for server. To install RHEL7 insert RHEL7 DVD in DVD-ROM and boot from DVD. After booting from DVD you would get following screen.

Select Install Red Hat system and press enter

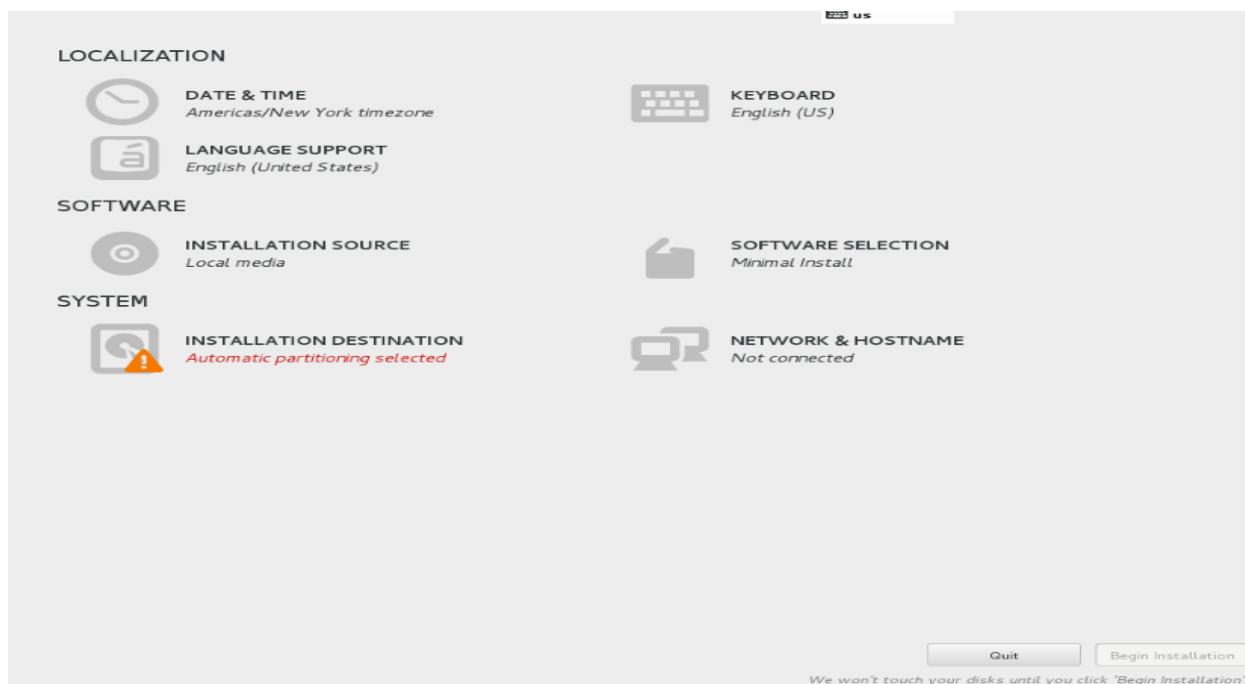


Installation process also would ask for a media check as shown above. Skip it

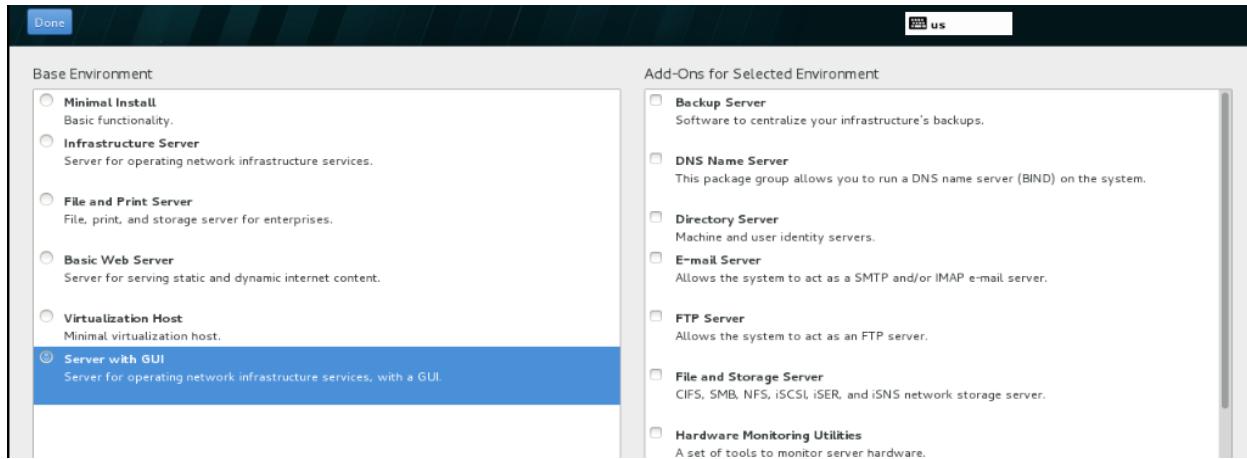
Depending on your hardware installation process would present welcome screen. If you have less resource you get command line or if you have sufficient hardware you would get graphic screen.



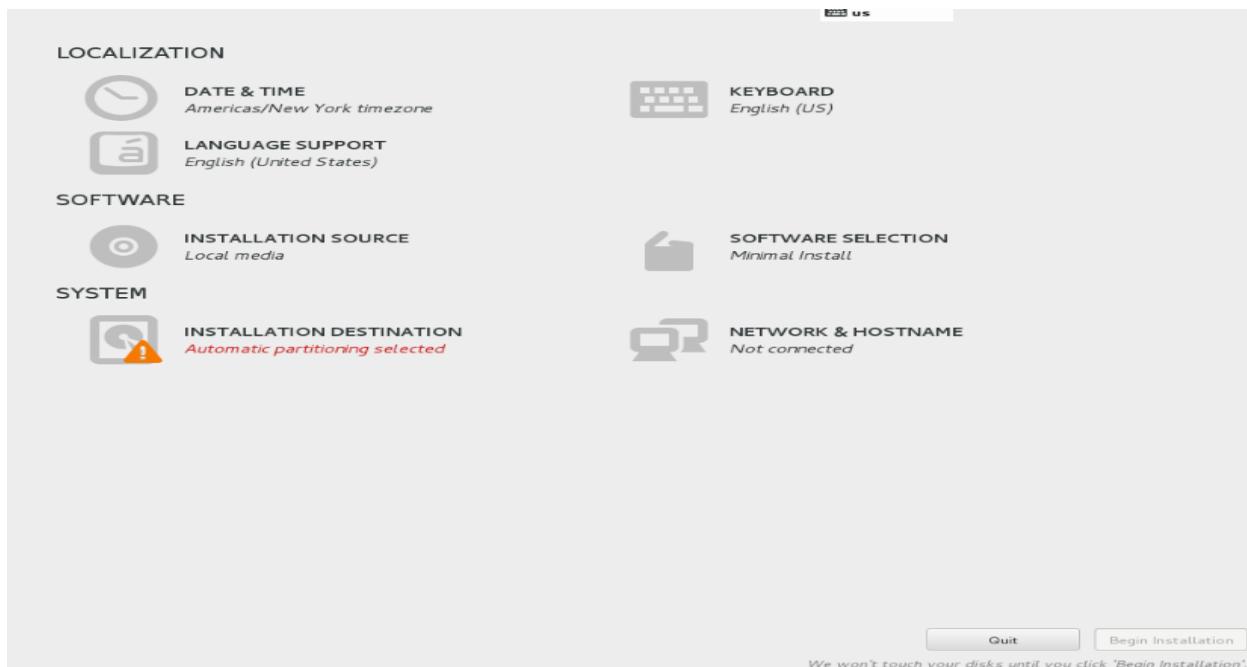
Select language and press okey then follow the given screenshot



Here there is no change required in localization section you need to change in Software section where you have to select Software selection and change default setting from Minimal install to Server with GUI



Now after selecting server with GUI press done button then you will be appeared for the previous screen



Now click on Installation destination then you will find the below screen



Done

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

15.36 GB Virtio Block Device vda / 15.36 GB free
--

Disks left unselected here will not be touched.

Specialized & Network Disks

Add a disk...

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

Automatically configure partitioning. I will configure partitioning.
 I would like to make additional space available.

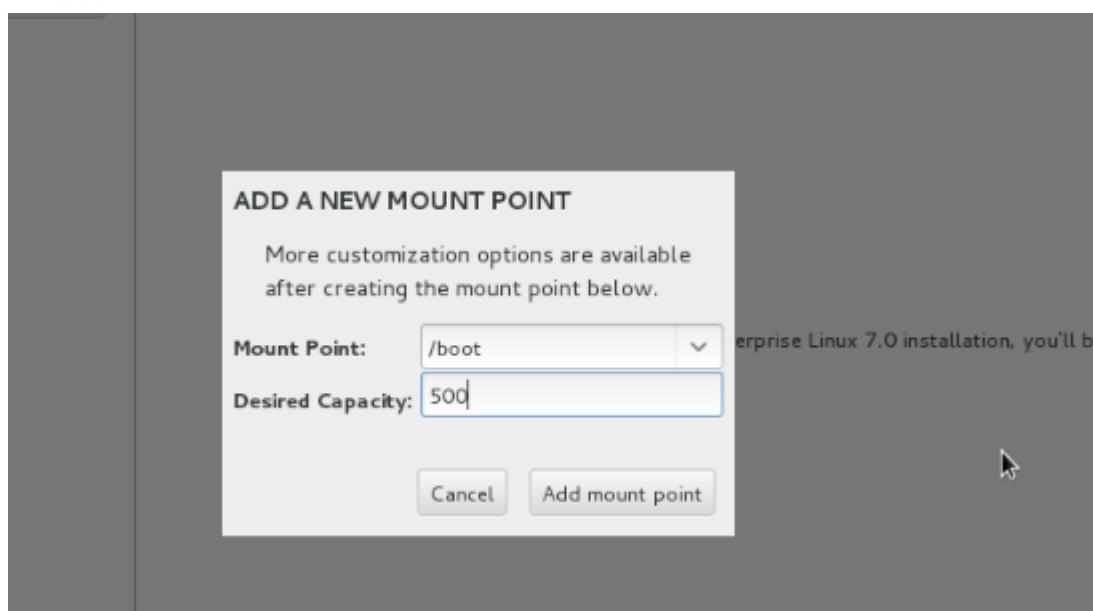
Encryption

Encrypt my data. You'll set a passphrase later.

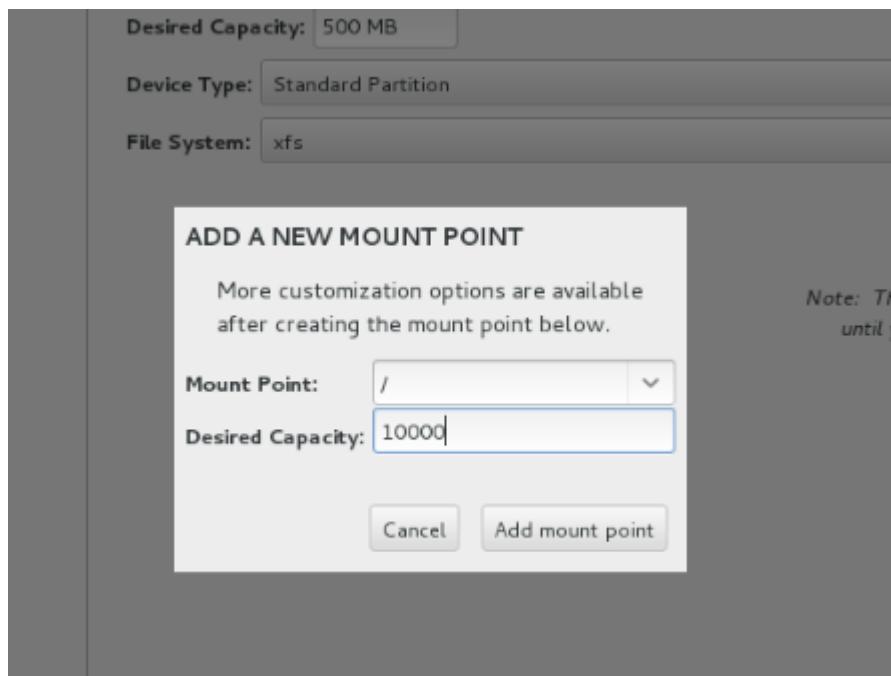
Select the I will configure partition and click on done button then you will fine below screen.



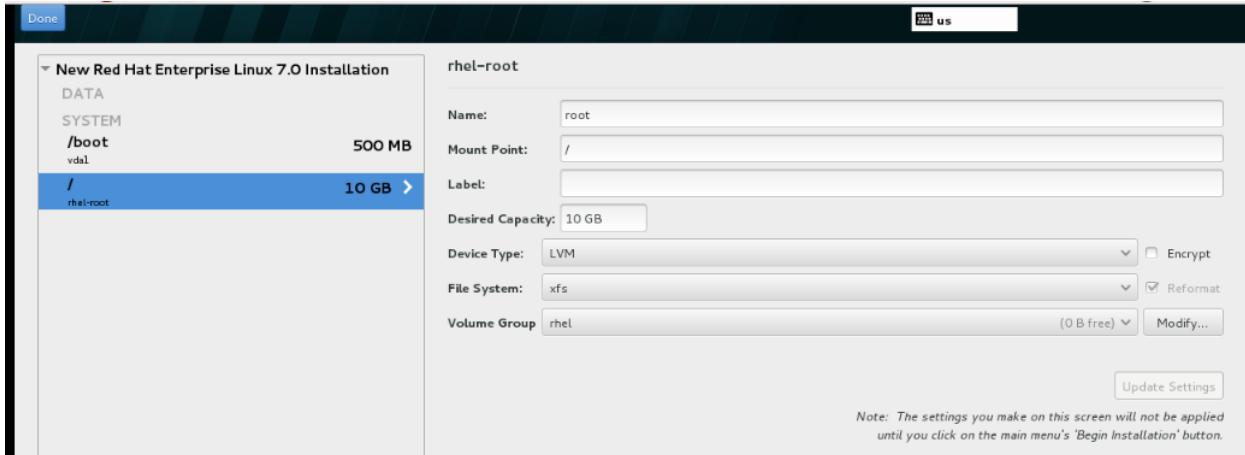
Note: here you will find free and available space now click on + sign to add a new a partition and you will appear like given below picture then made the entry



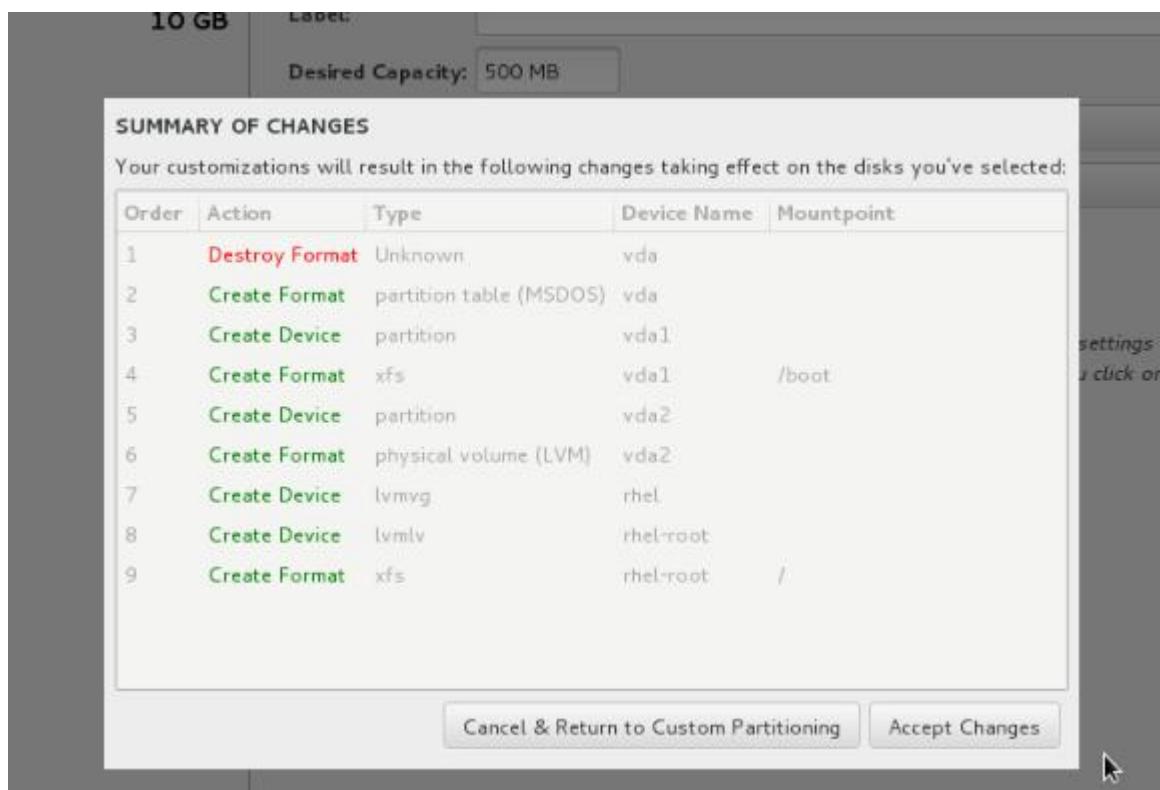
After adding mount point create one more partition to mount / as shown below



Follow the given step for more reference.

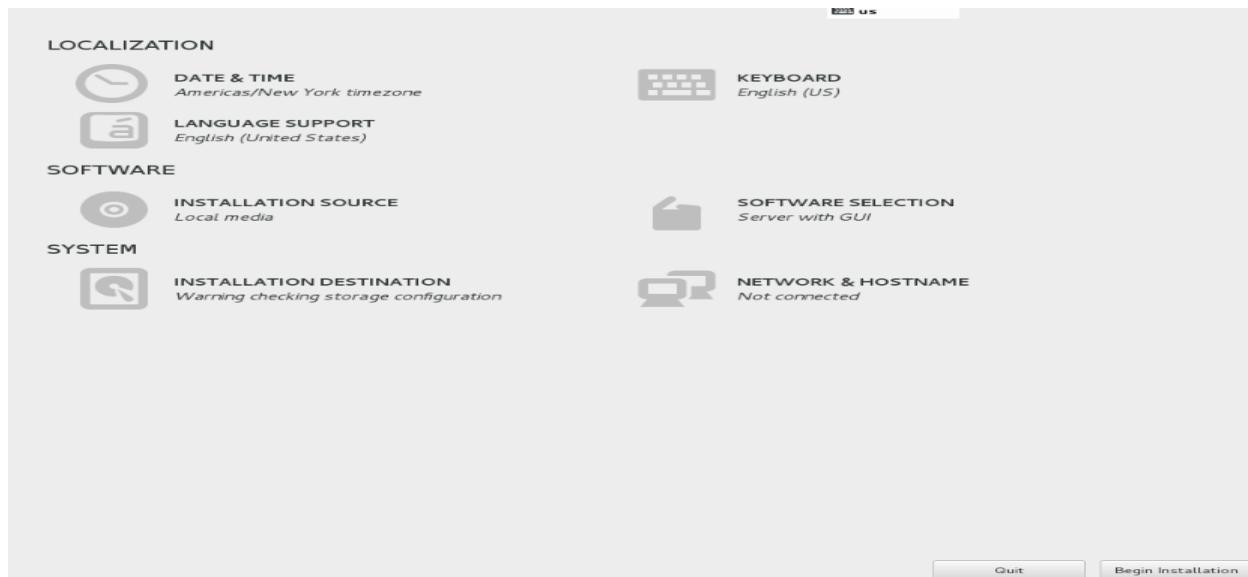


Now click on done button to proceed further.

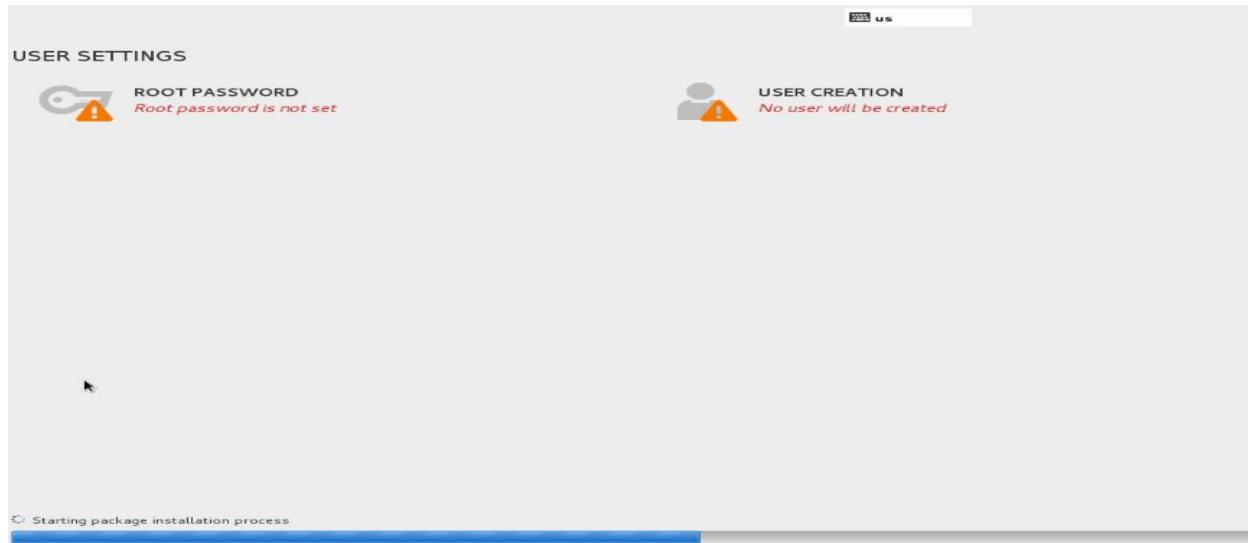


Click at accept changes.

By clicking begin installation you can start your installation process



Now set root password and create an account as option shown below





Done

The root account is used for administering the system. Enter a password for the root user.

Root Password: Weak

Confirm:

Also add user

Done

Full name

Username

Tip: Keep your username shorter than 32 characters and do not use spaces.

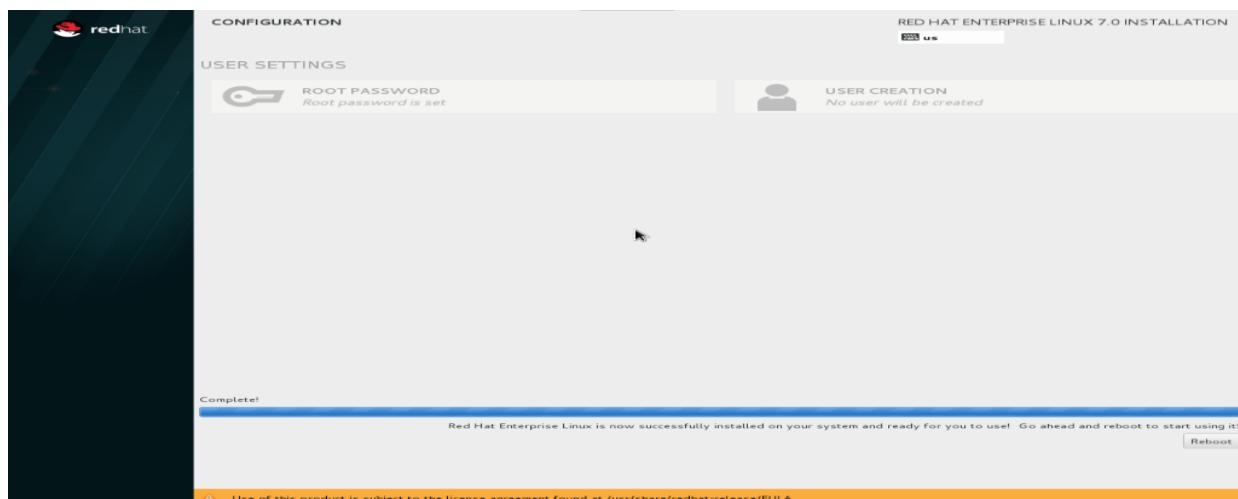
Make this user administrator

Require a password to use this account

Password Weak

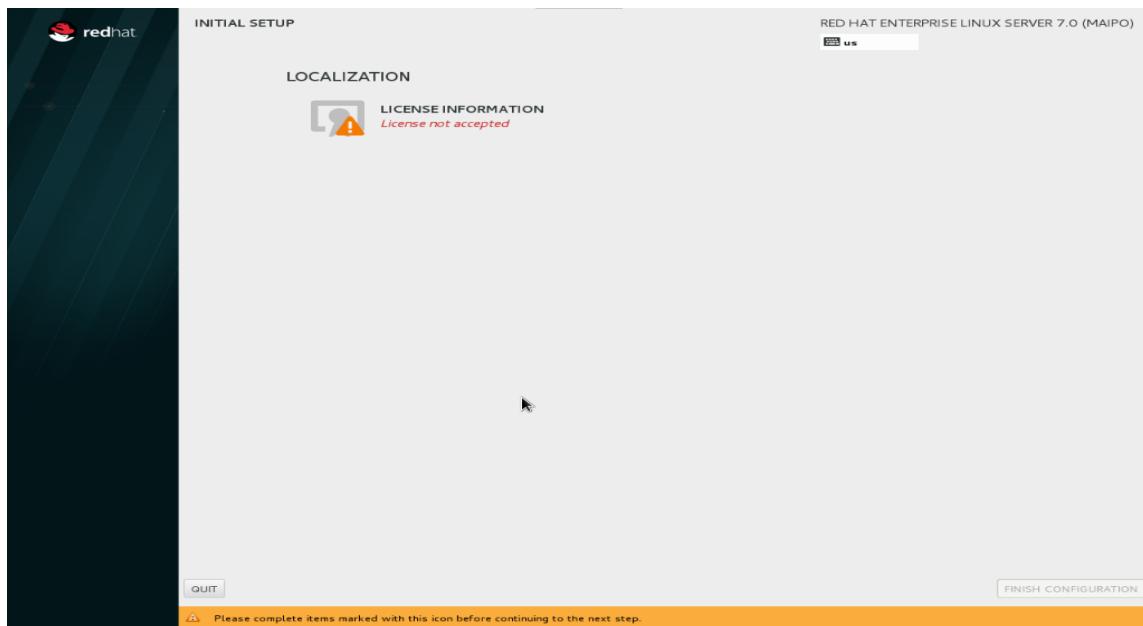
Confirm password

Once your installation is completed reboot your system as given button.

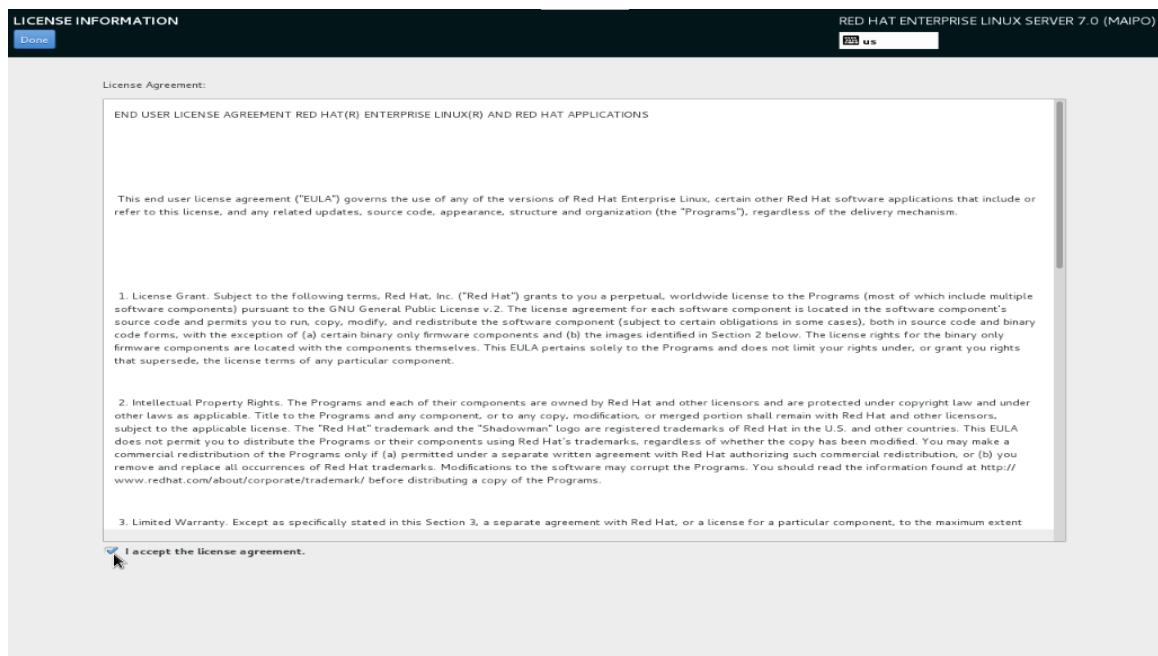




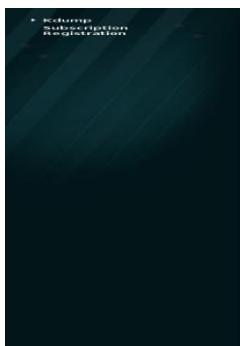
After reboot post install wizard would run. On welcome screen Click on forward



On license screen select yes I agree to the license agreement



Now you would get set up software updates screen. In real life you should set up software updates from RHN network. But in practice environments you could skip this step. select No I prefer to register at a later time and click on forward it would open a reminder pop up click on No thanks I will connect later



Kdump

Kdump is a kernel crash dumping mechanism. In the event of a system crash, it will automatically dump the memory state of the system, which is invaluable in determining the cause of the crash. Note that kdump does not affect the operation of system memory that will be unavailable for other processes.

Enable kdump?

Kdump Memory Reservation (MB):

Automatic

Manual

161

Memory To Be Reserved (MB):

130

197.9

338.0

Default System Interceptor (MB):

Advanced kdump configuration

This defines where to put the /var/crash/kdump files.

This file contains a series of commands to perform (in order) when a kernel crash has happened and the kdump kernel has been loaded. Directives in this file tell the kdump daemon what should be done and what should not be done. It is recommended to leave this file empty.

If the configured dump target fails, the default action will be performed.

Generally enter the target host and path may be required as follows:

If the configured dump target fails, the default action will be performed.

Basic commands supported area:

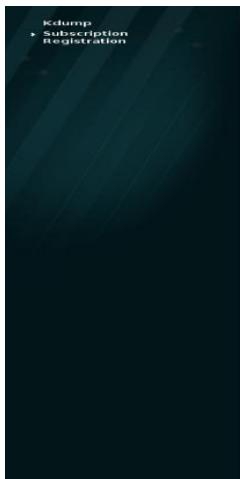
raw <partition> will dd /proc/meminfo into <partition>.

Use <partition> as device names for partition devices,

such as /dev/sda1.

nfs = nfs mount -> /mnt > /var/crash/kdump-*sdDATE/*, supports DNS.

[Back](#) [Forward](#)



Subscription Management Registration

This assistant will guide you through the process of registering your system with Red Hat to receive software updates, support, and other benefits. You will need the following to register:

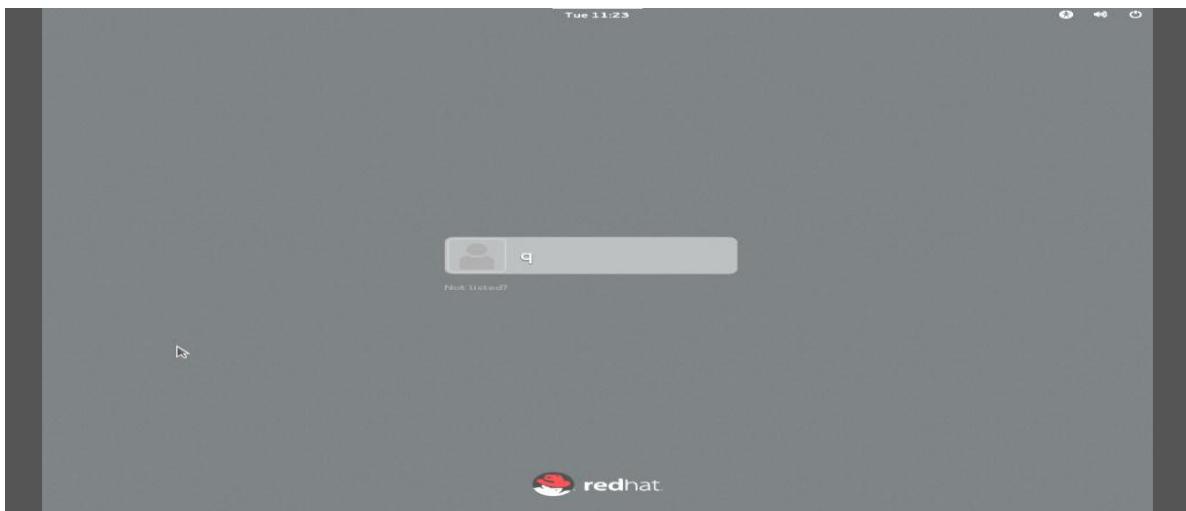
- A network connection
- Your account login
- The address of a subscription management service (optional)

[Why Should I Register?](#)

Would you like to register your system at this time? Yes, I'd like to register now. No, I prefer to register at a later time.

[Back](#) [Finish](#)

In a minute you would get default login screen.



Congratulations you have successfully installed RHEL7 from media.

Basic Command

In Linux everything is file and to manage these files Linux administrator use command line tools. In this section you will learn how to use command line tools to manage files. We would start from basic and extend it till RHCE exam level. You would learn how to login in command prompt, how to use Linux shell, how to use text editor in command line and many more.

From RHCE7 command line skills are combined with network configuration objectives. In this section we would try to cover those commands with example which requires in RHCE exam.

This section is good for beginner as well. We suggest you to go through with each articles of this section as linux administrators frequently use commands to perform administrate task.

Understanding command prompt

On a default Redhat system terminal consoles look like this.



```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64
server60 login:
```

Above image contain following information.

Release version of RHEL Red Hat Enterprise Linux Server release 7.0)

Version number of the kernel Kernel 2.6.32-131.0.15.el.x86_64 on an x86_64

System hostname Localhost

Which command line prompt are you going to get depends on user type. However you could customize the prompt. Linux systems have two types of user super user known as root user and normal user. For these Linux system have two basic prompts. The following is an example of what you might see when logged in as a normal user:

Note how it includes the username, the hostname of the local system, the current directory, and a \$ prompt. The \$ prompt is the standard for normal users.

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: vimal
Password:
Last login: Tue Apr 28 11:59:02 on tty3
[vimal@server86 ~]$ pwd
/home/vimal
[vimal@server86 ~]$
```

In above example

vimal Username

Localhost computer name

~ user's home directory in this example it would be /home/vimal Every user by default gets a directory in home folder.

Now take a look at a prompt for the root administrative user on the same system. It should look familiar. Except for the name of the account, the only consistent difference is the prompt.

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: root
Password:
[root@server86 ~]# whoami
root
[root@server86 ~]#
```

In this example

Root Username

Localhost computer name

~ user's home directory in this example it would be /root Root user get its directory separate from other users.

RHEL Terminal Emulation CLI Interface

In the early days of Linux (around 1990s) all that was available was a simple text interface to the Linux operating system. This text interface allowed administrators to start programs, control program operations, and move files around on the system.

With the popularity of Microsoft Windows, computer users expected more than the old text interface to work with. This spurred more development in the OSS community, and the Linux graphical desktops emerged.

Back before the days of graphical desktops, the only way to interact with a Unix system was through a text command line interface (CLI) provided by the shell. The CLI allowed text input only, and could only display text and rudimentary graphics output.

As you well know, things are significantly different in today's Linux environment. Just about every Linux distribution uses some type of graphical desktop environment. However, to access the shell you still need a text display to interact with a CLI.

Linux is famous for being able to do things in more than one way, and no place is this more relevant than in graphical desktops.

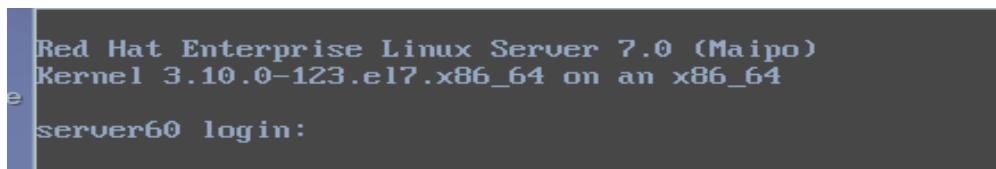
With all of the new graphical Linux desktop features, sometimes finding a way to get a CLI in a Linux distribution is an easy task.

One way to get to a CLI is to take the Linux system out of graphical desktop mode and place it in text mode. This provides nothing more than a simple shell CLI on the monitor, just like the days before graphical desktops. This mode is called the Linux console, since it emulates the old days of a hard-wired console terminal, and is a direct interface to the Linux system.

By default 6 command line consoles and one GUI console is available in Redhat system. They're defined in start-ttys.conf file in the /etc/init directory.

To change between consoles, press ALT and the function key associated with the console. For example, the ALT-F5 key combination moves to the five console.

In the RHEL GUI, the ALT-F2 key combination is used to start the Run Application tool; therefore, you'll need to press CTRL-ALT-F2 to move to that second virtual console.



```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.e17.x86_64 on an x86_64
server60 login:
```

At a text console login, you'd see the above prompt, which depends a bit on the release of RHEL, the version number of the kernel, and the system hostname:

File navigation in command line

New comer in Linux may prefer to use the GUI to manage Linux file system. But Linux administrator/ Linux professional use command line to manage Linux file system because command line tools give you ability to find your way around the every Linux distribution.

For RHCE certification you need some basic concepts of file navigation to find the important files. In this article I would show some basic command which you need in RHCE certification to navigate the RHEL system.

pwd

On a Linux you could easily find out the name of current directory. The **pwd** command identifies the current directory and prints the name of current directory. You can easily remember it as present working directory.

```
[root@localhost ~]# pwd
/root
[root@localhost ~]# _
```

cd

Simple command to change the directory.

```
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd test
[root@localhost test]# pwd
/root/test
[root@localhost test]# _
```

absolute and relatives path

before you start playing around the Linux file system be familiar and understand the difference between absolute and relative path.

An absolute path describes the complete directory structure in terms of the top-level directory, root (/).

A relative path is based on the current directory. Relative paths do not include the slash in front.

Let take a simple example to understands distinguish between absolute and relative path.

You are logged in from root user and want to go in /home/sanjay directory

Form relative path

```
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /home/sanjay/
[root@localhost sanjay]# pwd
/home/sanjay
[root@localhost sanjay]# _
```

From absolute path

```
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /home/sanjay/
[root@localhost sanjay]# pwd
/home/sanjay
[root@localhost sanjay]# _
```

Tilde (~)

On Linux system every user after successful login is taken to his home directory. The tilde (~) is used to represent the home directory of any currently active user.

For example, when user sanjay logs in, he's taken to his home directory, /home/vimal.

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: vimal
Password:
Last login: Tue Apr 28 11:59:02 on tty3
[vimal@server86 ~]$ pwd
/home/vimal
[vimal@server86 ~]$
```

In contrast, the home directory of the root administrative user is /root.

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: root
Password:
Last login: Tue Apr 28 12:05:49 on tty3
[root@server86 ~]$ pwd
/root
[root@server86 ~]$
```

To return in home directory from anywhere in file system

Use cd command without any argument.

```
[root@localhost var]# pwd
/var
[root@localhost var]# cd
[root@localhost ~]# pwd
/root
[root@localhost ~]# _
```



It's not necessary but you could pass ~ with cd command to return the home directory of user.

```
[root@localhost ~]# pwd  
/var  
[root@localhost ~]# cd ..  
[root@localhost ~]# pwd  
/root  
[root@localhost ~]# _
```

Thus, the effect of the `cd ~` command depends on your username.

For example, if you've logged in as user sanjay, the `cd ~` command navigates to the `/home/sanjay` directory.

If you've logged in as the root user, this command navigates to the /root directory.

Listing the content of directory

Ls command is helpful to see what files exist in a directory.

```
[root@localhost ~]# ls  
anaconda-ks.cfg  Documents  install.log      Music  
Desktop          Downloads  install.log.syslog Pictures  
[root@localhost ~]# -
```

Ls command with the right switches, can be quite powerful.

ls -a :- to reveal hidden files

```
[root@localhost ~]# ls -a
.. .dock .groups Music
. .Desktop .gstreamer-0.10 .nautilus
.anaconda-ks.cfg .Documents .gtk-bookmarks Pictures
.bash_history .Downloads .gvfs Public
.bash_logout .esd_auth .ICEauthority .pulse
.bash_profile .xconf icons .pulse-cookie
.bashrc .xconfd install.log .spice-vdagent
.config .xorg .gnome2 install.log.syslog .ssh
.cshrc .xpi .local tcshrc
[root@localhost ~]# _
```

Is -l :- for long listings

```
[root@localhost ~]# ls -l
total 96
-rw-----. 1 root root 2405 Jul 21 01:31 anaconda-ks.cfg
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Desktop
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Documents
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Downloads
-rw-r--r--. 1 root root 38630 Jul 21 01:31 install.log
-rw-r--r--. 1 root root 9888 Jul 21 01:27 install.log.syslog
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Music
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Pictures
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Public
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Templates
drwxr-xr-x 2 root root 4096 Jul 22 01:45 test
drwxr-xr-x 2 root root 4096 Jul 20 20:52 Videos
[root@localhost ~]# _
```

ls -t :- for a time-based list

```
[root@localhost ~]# ls -lt
total 96
drwxr-xr-x. 2 root root 4096 Jul 22 01:45 test
-rw-----. 1 root root 2405 Jul 21 01:31 anaconda-ks.cfg
-rw-r--r--. 1 root root 38630 Jul 21 01:31 install.log
-rw-r--r--. 1 root root 9888 Jul 21 01:27 install.log.syslog
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Desktop
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Documents
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Downloads
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Music
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Pictures
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Public
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Templates
drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Videos
[root@localhost ~]# _
```

ls -i :- for inode numbers

```
[root@localhost ~]# ls -li
total 96
537342 -rw-----. 1 root root 2405 Jul 21 01:31 anaconda-ks.cfg
12867 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Desktop
12871 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Documents
12868 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Downloads
519171 -rw-r--r--. 1 root root 38630 Jul 21 01:31 install.log
519173 -rw-r--r--. 1 root root 9888 Jul 21 01:27 install.log.syslog
12872 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Music
12873 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Pictures
12870 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Public
12869 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Templates
519188 drwxr-xr-x. 2 root root 4096 Jul 22 01:45 test
12874 drwxr-xr-x. 2 root root 4096 Jul 20 20:52 Videos
[root@localhost ~]# _
```

ls -Z :- The system_u, object_r, var_t, and s0 output demonstrates the current SELinux contexts of the noted files. During the RHCE you will be expected to configure a system with SELinux enabled.

```
[root@localhost ~]# ls -Z
-rw-----. root root system_u:object_r:admin_home_t:s0 anaconda-ks.cfg
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Desktop
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Documents
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Downloads
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 install.log.syslog
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Music
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Pictures
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Public
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Templates
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 test
drwxr-xr-x. root root unconfined_u:object_r:admin_home_t:s0 Videos
[root@localhost ~]# _
```

Basic commands to manage files

Linux and Unix are managed through a series of text files. Linux administrators do not normally use graphical editors to manage these configuration files. Editors such as WordPerfect, OpenOffice.org Writer, Microsoft Word normally either save files in a binary format or add tags. Unless text files are preserved in their original format, without tags, changes that are made can render a Linux system unbootable.

In RHCE certification you have to perform several tasks on command line. In this article I would some basic commands to create / edit /delete files on Linux system.

How to create and read files on command line in RHEL Linux

Everything in Linux can be reduced to a file.

cat

The most basic command for reading and creating files is **cat**. The cat filename command scrolls the text within the filename file. It also works with multiple filenames; it concatenates the filenames that you might list as one continuous output to your screen. You can redirect the output to the filename of your choice.

To Create a file

```
[sanjay@localhost ~]$ cat > file1
This is 1 line in file1
Now we are in 2 line we can not go back in line1
Press d with ctrl key to save file
Do not press d with ctrl key second time as on
first time file would be saved and you would return
to command prompt and if you press again ctrl d it would
logged you out. ctrl + d is the short cut key of logged out on
command prompt
[sanjay@localhost ~]$ _
```

Use ctrl+d to save file

To read the contain of file

```
[sanjay@localhost ~]$ ls
file1
[sanjay@localhost ~]$ cat file1
This is 1 line in file1
Now we are in 2 line we can not go back in line1
Press d with ctrl key to save file
Do not press d with ctrl key second time as on
first time file would be saved and you would return
to command prompt and if you press again ctrl d it would
logged you out. ctrl + d is the short cut key of logged out on
command prompt
[sanjay@localhost ~]$ _
```

To extend the contain of file use >> with cat command

```
[sanjay@localhost ~]$ cat >> file1
This line would be added in the file1
[sanjay@localhost ~]$ cat file1
This is 1 line in file1
Now we are in 2 line we can not go back in line1
Press d with ctrl key to save file
Do not press d with ctrl key second time as on
first time file would be saved and you would return
to command prompt and if you press again ctrl d it would
logged you out. ctrl + d is the short cut key of logged out on
command prompt
This line would be added in the file1
[sanjay@localhost ~]$ _
```

While extending contents from cat command take care of > . User single > to create new file and >> to extend the contents. If you have used single > to extended the content it would overwrite the existing content of file without any warning.

```
[sanjay@localhost ~]$ cat > file1
This time as i am using single > to append
the content of file. It would overwrite the existing
content of file1.
[sanjay@localhost ~]$ cat file1
This time as i am using single > to append
the content of file. It would overwrite the existing
content of file1.
[sanjay@localhost ~]$ _
```

How to create directories on command line in RHEL Linux

Directories are special types of files that serve as containers for other files.

mkdir

Basic command to create new directory.

```
[sanjay@localhost ~]$ ls
file1
[sanjay@localhost ~]$ mkdir dir1
[sanjay@localhost ~]$ ls
dir1  file1
[sanjay@localhost ~]$ _
```

To create directory tree use -p

```
[sanjay@localhost ~]$ ls
    file1
[sanjay@localhost ~]$ mkdir -p dir2/dir_a/dir_b/dir_c
[sanjay@localhost ~]$ ls
    file1
[sanjay@localhost ~]$ cd dir2
[sanjay@localhost dir2]$ ls

[sanjay@localhost dir2]$ cd dir_a
[sanjay@localhost dir_a]$ cd dir_b
[sanjay@localhost dir_b]$ cd dir_c
[sanjay@localhost dir_c]$ pwd
/home/sanjay/dir2/dir_a/dir_b/dir_c
[sanjay@localhost dir_c]$ _
```

How to delete files / directories on command line in RHEL Linux

To remove directory use **rmdir** command

```
[sanjay@localhost ~]$ ls
dir1 dir2
[sanjay@localhost ~]$ rmdir dir1
[sanjay@localhost ~]$ ls
dir2
[sanjay@localhost ~]$ rmdir dir2
rmdir: failed to remove 'dir2': Directory not empty
[sanjay@localhost ~]$ _
```

To delete file use **rm** command

```
[sanjay@localhost ~]$ ls
dir1 dir2  file1
[sanjay@localhost ~]$ rm file1
[sanjay@localhost ~]$ ls
dir1  dir2
[sanjay@localhost ~]$ _
```

rmdir command would not delete a directory which contain data inside it

To delete a directory which contain data inside it use **rm** command with **-rf** option

```
[sanjay@localhost ~]$ rm -rf dir2
[sanjay@localhost ~]$ ls
[sanjay@localhost ~]$ _
```

Reading the content of file

From our earlier articles of this section you have learnt how to create files and directories. You have also played around the Linux file system. Now its time to read contents of files with some advance options.

less and more

Everything in Linux is file. Sometime you may find its very hard to read the entire file. To navigate in the file Linux provide some cool commands.

Linux has two of these commands: more and less. With the more filename command,

```
[root@localhost ~]# more /var/log/messages
```

you can scroll through the text of a file, from start to finish, one screen at a time.

With the less filename command,

```
[root@localhost ~]# less /var/log/messages
```

you can scroll in both directions. Use PAGE UP and PAGE DOWN keys to scroll.

Press **q** anytime to quit from the output of the commands.

During the exam sometime you need to find some text in files. Like in configuration files you need to find some configuration values. Or you may need to locate some error in error log files.

As the less and more commands do not change files, they are an excellent way to scroll through and search for items.

Let take a example

open /var/log/messages file with less command

```
[root@localhost ~]# less /var/log/messages
```

Now I would search the term "pwd_max", in forward

```
Jul 21 02:14:31 localhost
(reserved)
Jul 21 02:14:31 localhost
(reserved)
Jul 21 02:14:31 localhost
(reserved)
/pwd_max_
```

To search in the reverse direction, substitute a ? for the /.

```
Jul 21 02:14:31 localhost
? pid_max_
```

Found string would be shown like this

```
Jul 21 02:14:31 localhost kernel: pid_max: default: 32768 minimum: 301
Jul 21 02:14:31 localhost kernel: Security Framework initialized
Jul 21 02:14:31 localhost kernel: SELinux: Initializing.
Jul 21 02:14:31 localhost kernel: Dentry cache hash table entries: 131072
[ 8 1048576 kbytes]
```

With more command you could only search in forward direction.

One more cool feature of less command is it could read the in Gzip format compress files without uncompressing them.

This features only available in less commands

Gzip format, normally shown with the .gz extension.

```
[root@localhost ~]# less /usr/share/man/man1/cat.1.gz
```

Viewing parts of a file

Often the data you want to view is located either right at the top or buried at the bottom of a text file. If the information is at the top of a large file, you still need to wait for the cat or more commands to load the entire file before you can view it. If the information is located at the bottom of a file (such as a log file), you need to wade through thousands of lines of text just to get to the last few entries. Fortunately, Linux has specialized commands to solve both of these problems.

[head and tail](#)

The **tail** command

displays the last group of lines in a file. By default, it will show the last 10 lines in the file.

```
[root@localhost ~]# tail /var/log/messages
Jul 22 05:39:37 localhost NetworkManager[1303]: <info>      gateway 192.168.219.2
Jul 22 05:39:37 localhost NetworkManager[1303]: <info>      nameserver '192.168.219
.2'
Jul 22 05:39:37 localhost NetworkManager[1303]: <info>      domain name 'localdomain'
Jul 22 05:39:37 localhost avahi-daemon[1320]: Withdrawing address record for 192
.168.219.130 on eth0.
Jul 22 05:39:37 localhost avahi-daemon[1320]: Leaving mDNS multicast group on in
terface eth0.IPv4 with address 192.168.219.130.
Jul 22 05:39:37 localhost avahi-daemon[1320]: Interface eth0.IPv4 no longer rele
vant for mDNS.
Jul 22 05:39:37 localhost avahi-daemon[1320]: Joining mDNS multicast group on in
terface eth0.IPv4 with address 192.168.219.131.
Jul 22 05:39:37 localhost avahi-daemon[1320]: New relevant interface eth0.IPv4 f
or mDNS.
Jul 22 05:39:37 localhost avahi-daemon[1320]: Registering new address record for
192.168.219.131 on eth0.IPv4.
Jul 22 05:39:38 localhost NetworkManager[1303]: <info> Policy set 'System eth0'
(eth0) as default for IPv4 routing and DNS.
[root@localhost ~]# _
```

but you can change it with -n switch. For example to see the 2 line use

```
[root@localhost ~]# tail -2 /var/log/messages
Jul 22 05:39:37 localhost avahi-daemon[1320]: Registering new address record for
192.168.219.131 on eth0. IPv4.
Jul 22 05:39:38 localhost NetworkManager[1303]: <info> Policy set 'System eth0'
(eth0) as default for IPv4 routing and DNS.
[root@localhost ~]# _
```

The head command

While not as exotic as the tail command, the head command does what you would expect, it displays the first group of lines at the start of a file. By default, it will display the first 10 lines of text.

```
[root@localhost ~]# head /var/log/messages
Jul 21 02:14:31 localhost kernel: imklog 4.6.2, log source = /proc/kmsg started.
Jul 21 02:14:31 localhost rsyslogd: [origin software="rsyslogd" swVersion="4.6.2
" x-pid="1241" x-info="http://www.rsyslog.com"] (re)start
Jul 21 02:14:31 localhost kernel: Initializing cgroup subsys cpuset
Jul 21 02:14:31 localhost kernel: Initializing cgroup subsys cpu
Jul 21 02:14:31 localhost kernel: Linux version 2.6.32-131.0.15.el6.x86_64 (mock
build0x86-007.build.bos.redhat.com) (gcc version 4.4.4 20100726 (Red Hat 4.4.4-1
3) (GCC) ) #1 SMP Tue May 10 15:42:40 EDT 2011
Jul 21 02:14:31 localhost kernel: Command line: ro root=UUID=287b57d9-4db9-40ff-
9d6a-3a438b280a7b rd_NO_LUKS rd_NO_LVM rd_NO_MD rd_NO_DM LANG=en_US.UTF-8 SYSFON
T=latarcyrheb-sun16 KEYBOARDTYPE=pc KEYTABLE=us crashkernel=auto quiet
Jul 21 02:14:31 localhost kernel: KERNEL supported cpus:
Jul 21 02:14:31 localhost kernel: Intel GenuineIntel
Jul 21 02:14:31 localhost kernel: AMD AuthenticAMD
Jul 21 02:14:31 localhost kernel: Centaur CentaurHauls
[root@localhost ~]# _
```

Similar to the tail command, you can use -n switch

```
[root@localhost ~]# head -n 2 /var/log/messages
Jul 21 02:14:31 localhost kernel: imklog 4.6.2, log source = /proc/kmsg started.
Jul 21 02:14:31 localhost rsyslogd: [origin software="rsyslogd" swVersion="4.6.2
" x-pid="1241" x-info="http://www.rsyslog.com"] (re)start
[root@localhost ~]# _
```

Linux Environment Variables

In this article we would understand linux environment variables. Environmental variable plays significant role in linux system.

We would cover following topics in this article

What is a linux environment variable

How to show linux environment variable

How to set linux environment variable

How to set linux environmental variable permanently

List of Linux environmental variable

What is a linux environment variable

Linux environment variable is an object that contains value. In simple terms it is a pair of data object and their respective values. If you are familiar with programming language than you can easily understand it. Linux environment variables do same job which variables do in programming language.

If you are not familiar with programming language you can understand linux variable as a container with name which keeps value inside it. This value could be location of all executable files in the filesystem, the default editor that should be used, or the system locale settings.

Example of linux environmental variable

Let take a simple example of **ls** command to understand linux environmental variables. **ls** the basic command to list the content of directory. When execute a command in linux, you need to type the full path of that command. Since the **ls** command is in the **/bin** directory, users should execute the **/bin/ls** command to list files in the current directory.

Here comes the magic of linux environmental variables. Linux have a PATH variable. With the help of the PATH variable, full path is not required. The bash shell automatically searches through the directories listed in a user's PATH variable for the command that user just typed at the command line. When a matching command found shell run it. In this way environment variable provides a simple way to share configuration settings between multiple applications and processes in Linux.

How to show linux environment variable

printenv or **env** command can be use to list linux environment variables. The **coreutils** package contains **printenv** and **env**. Use **printenv** command to show linux environmental variables.

```
$ printenv
```



LINUXWORLD™

[user1@server ~]\$ printenv_



ISO 9001:2008 CERTIFIED ORGANISATION

The **env** utility can also be used to show linux environment variables.

\$env

[user1@server ~]\$ env

printenv to print the names and the values of each. Note that some environment variables are user-specific. Output of **env** and **printenv** are too big to fit in screen. We can redirect the output of **printenv** in a file. To redirect the output of **printenv** in a file run following command

\$printenv > tmp_file

[user1@server ~]\$ printenv > tmp_file
[user1@server ~]\$ _

now we can read the tmp_file with less command.

\$less tmp_file

[user1@server ~]\$ printenv > tmp_file
[user1@server ~]\$ less tmp_file

Use up arrow and down arrow key to scroll. Press **q** to exist from file

```
HOSTNAME=server.example.com
TERM=linux
SHELL=/bin/bash
HISTSIZE=1000
XDG_SESSION_COOKIE=b5bd23c216a40532b967cf2
QTDIR=/usr/lib64/qt-3.3
QTINC=/usr/lib64/qt-3.3/include
USER=user1
LS_COLORS=rs=0:di=01:34:ln=01:36:mh=00:pi=
=48:33:01:or=40:31:01:mi=01:05:37:41:su=37
```

After reading you can simple remove the temporary file

\$rm tmp_file

```
HOME=/home/user1
LOGNAME=user1
QTLIB=/usr/lib64/qt-3.3/lib
CUS_RSH=ssh
LESSOPEN=t/usr/bin/lesspipe.sh %s
G_BROKEN_FILERENAMES=1
=/usr/bin/printenv
[user1@server ~]$ rm tmp_file
[user1@server ~]$
```

How to set linux environment variable

Linux environment can be set in three ways.

Temporary also known as Session Specific Variables

permanent locally

Permanent globally

To set linux environmental variable temporary use **export** command.

PATH variable contains location of executable files. To check current **PATH** use following command

```
$ echo $PATH
```

```
[user1@server ~]$ echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/user1/bin
[user1@server ~]$ _
```

Now we would add our directory in this path. Make a directory

```
$mkdir custom_script
```

To add this directory in path run following commands

```
$export PATH="${PATH}:/home/user1/custom_script"
```

Verify that we have successfully added our *custom_script* directory in **PATH** variable

```
[user1@server ~]$ echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/user1/bin
[user1@server ~]$ mkdir custom_script
[user1@server ~]$ export PATH="${PATH}:/home/user1/custom_script"
[user1@server ~]$ echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/user1/bin:/home/user1/custom_script
[user1@server ~]$ _
```

Now move in our *custom_script* directory and make a sample script

```
[user1@server custom_script]$ cat > simple_script
echo "Hello world "
[user1@server custom_script]$ _
```

make *sample_script* executable and run script directly from command prompt.

```
[user1@server custom_script]$ cat > simple_script
echo "Hello World"
[user1@server custom_script]$ chmod +x simple_script
[user1@server custom_script]$ simple_script
Hello World
[user1@server custom_script]$ _
```

You can also verify that shell run *sample_script* from our *custom_script* directory by which command

```
[user1@server custom_script]$ cat > simple_script
echo "Hello World"
[user1@server custom_script]$ chmod +x simple_script
[user1@server custom_script]$ simple_script
Hello World
[user1@server custom_script]$ which simple_script
~/custom_script/simple_script
[user1@server custom_script]$ ls
simple_script
[user1@server custom_script]$ _
```

Temporary variable only available in current session. To test it log out from current user and login back.

Run *sample_script* again. This time you will get command not found error.

```
[user1@server ~]$ cd custom_script/
[user1@server custom_script]$ ls
simple_script
[user1@server custom_script]$ simple_script
-bash: simple_script: command not found
[user1@server custom_script]$ _
```

How to set linux environmental variable permanently

Defining Variables Locally

As you seen temporary variables are available only on that session. We can make those variables permanent. For security reason you should not define an environment variable globally unless you have sound understanding of linux system. For instance, you might want to add */home/user_name/custom_script* to the **PATH** variable for a particular user. In such a case define it locally. As you do not want all other users on your system to have that in their PATH too.

The following files should be used for local environment variables on your system: `~/.profile`, `~/.bash_profile`, `~/.bash_login` and `~/.bash_logout`.

```
[user1@server ~]$ ls -a
.  ..  .bus  .ICEauthority  .pulse-cookie
  .bash_history  .Desktop  .local  .recently-used.xbel
  .bash_logout  .Downloads  .mozilla  .pulseCookie
  .bash_profile  .esd_auth  .Music  .pulseCookie
  .bashrc  .gnome  .nautilus  .pulseCookie
  .cache  .gnome-d  .Pictures  .pulseCookie
  .config  .gnome2  .Public  .Xauthority
  custom_script  .gtk-bookmarks  .pulseCookie
  .pulseCookie
[user1@server ~]$ _
```

To add our `custom_script` directory in to the PATH variable for local usage

open `.bash_profile` file

```
vi ~/.bash_profile
custom_script  .gnome  .recently-used.xbel
  .bus  .ICEauthority  .pulseCookie
[user1@server ~]$ vi .bash_profile _
```

add our directory `/home/user1/custom_script` in PATH variable

```
#!/bin/bash
# Get the aliases and functions
if [ -f "$HOME/.bashrc" ]; then
    . "$HOME/.bashrc"
fi

# User specific environment and startup programs
PATH=$PATH:$HOME/bin:/home/user1/custom_script
export PATH
: wq_
```



To update the variable, re-login required.

Logout

```
[user1@server ~]$ exit_
```

Login back

Now check that our custom path is available

```
Red Hat Enterprise Linux Server release 6.1 (Santiago)
Kernel 2.6.32-131.8.15.el6.x86_64 on an x86_64

server login: user1
Password:
Last login: Wed Sep 12 06:42:59 on tty2
[user1@server ~]$ cd custom_script
[user1@server custom_script]$ simple_script
Hello World
[user1@server custom_script]$ echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/user1/bin:/home/user1/custom_script
[user1@server custom_script]$
```

Permanently set linux environmental variable Globally

root privilege requires to set linux environment variable globally. RHEL maintain and manage the environment variables in numerous files. But you do not need to pay attentions on all files that can contain environment variables. Following the RHEL recommendation you should only set environmental variables in some particular files. The following files should be used for defining global environment variables on your system: /etc/profile, /etc/bash.bashrc and /etc/environment.

/etc/profile.d Directory is used to define global script.

Login from root and move to /etc

```
Red Hat Enterprise Linux Server release 6.1 (Santiago)
Kernel 2.6.32-131.8.15.el6.x86_64 on an x86_64

server login: root
Password:
Last login: Wed Sep 12 08:29:55 on tty2
[root@server ~]# cd /etc
[root@server etc]#
```

move to /etc/profile.d directory

Make a simple test script and make this script executable

```
[root@server etc]# cd profile.d
[root@server profile.d]# cat > global_script.sh
echo "Hello World Globally variable"
[root@server profile.d]# chmod +x global_script.sh
[root@server profile.d]#
```

This script print a simple welcome message for all users

To test it logout from root and login back from normal user

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: vimal
Password:
Last login: Tue Apr 28 11:59:02 on tty3
[vimal@server86 ~]$ pwd
/home/vimal
[vimal@server86 ~]$
```

We have successfully added global script. After testing to remove it login back from root remove our test script

```
Red Hat Enterprise Linux Server release 6.1 (Santiago)
Kernel 2.6.32-131.0.15.el6.x86_64 on an x86_64

server login: root
Password:
Last login: Wed Sep 12 08:30:02 on tty2
Hello World Globally Variable
[root@server ~]# rm /etc/profile.d/global_script.sh
rm: remove regular file '/etc/profile.d/global_script.sh'? y
[root@server ~]# _
```

List of Linux environmental variable

Variable name	Stored information
DISPLAY	used by the X Window system to identify the display server
DOMAIN	domain name
EDITOR	stores your favorite line editor
HISTSIZE	size of the shell history file in number of lines
HOME	path to your home directory
HOSTNAME	local host name
INPUTRC	location of definition file for input devices such as keyboard
LANG	preferred language
LD_LIBRARY_PATH	paths to search for libraries

LOGNAME	login name
MAIL	location of your incoming mail folder
MANPATH	paths to search for man pages
OS	string describing the operating system
OSTYPE	more information about version etc.
PAGER	used by programs like man which need to know what to do in case output is more than one terminal window.
PATH	search paths for commands
PS1	primary prompt
PS2	secondary prompt
PWD	present working directory
SHELL	current shell
TERM	terminal type
UID	user ID
USER(NAME)	user name
VISUAL	your favorite full-screen editor
XENVIRONMENT	location of your personal settings for X behavior
XFILESEARCHPATH	paths to search for graphical libraries

Linux alias command

In this article we would use alias command. Default aliases provide safety features. For a Linux system administrator it is a handy tool.

How to check default alias

To check default alias run following command

```
$alias
```

```
[user1@server ~]$ alias
alias l='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias vi='vim'
alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot --show-ti
lde'
[user1@server ~]$ _
```

Some of the aliases listed are likely to be system-wide aliases that apply to all users and are created automatically for each new user for a particular shell. Aliases for any other shell can be seen by first switching to that shell and then using the alias command as above.

alias command allows you to launch any command or group of commands with simple names or abbreviations.

Syntax of alias is

```
alias name="value"
```

name is the name of the new alias

value is the command(s) which it initiates.

No spaces are permitted before or after the equals sign. Any number of aliases can be created simultaneously by enclosing the name in each name-value pair in quotes.

The alias name and the replacement text can contain any valid shell input except for the equals sign (=).

The commands, including any options, arguments and redirection operators, are all enclosed within a single pair of quotation marks, which can be single quotes or double quotes.

Take a simple example of **ls** command. **ls** command list the content of directory.

```
[user1@server ~]$ ls
custom_script  Documents  Music    Public      tmp
Desktop        Downloads  Pictures  Templates  Videos
[user1@server ~]$ _
```

With **-l** switch it list content in long format with details

```
[user1@server ~]$ ls
custom_script  Documents  Music    Public    tmp
Desktop        Downloads  Pictures  Templates  Videos
[user1@server ~]$ ls -l
total 21
drwxrwxr-x. 2 user1 user1 1024 Sep 12 06:41 custom_script
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Desktop
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Documents
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Downloads
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Music
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Pictures
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Public
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Templates
-rw-rw-r--. 1 user1 user1 1911 Sep 12 06:46 tmp
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Videos
[user1@server ~]$ _
```

With the use of **alias** command we can create an alias for **ls** command with **-l** switch so when you run **ls** command it execute with **-l** switch

```
[user1@server ~]$ alias ls="ls -l"
[user1@server ~]$ ls
total 21
drwxrwxr-x. 2 user1 user1 1024 Sep 12 06:41 custom_script
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Desktop
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Documents
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Downloads
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Music
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Pictures
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Public
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Templates
-rw-rw-r--. 1 user1 user1 1911 Sep 12 06:46 tmp
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Videos
[user1@server ~]$ _
```

You can use any simple easy to remember name instead of command and than use them in the same way that ordinary commands are used.

For example you can use **list** keyword

```
[user1@server ~]$ alias list="ls -l"
[user1@server ~]$ list
total 21
drwxrwxr-x. 2 user1 user1 1024 Sep 12 06:41 custom_script
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Desktop
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Documents
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Downloads
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Music
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Pictures
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Public
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Templates
-rw-rw-r--. 1 user1 user1 1911 Sep 12 06:46 tmp
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Videos
[user1@server ~]$ _
```

alias set in this way are known temporary alias. Temporary alias would not be available after logout.

How to make alias permanent

You can make alias permanent locally and globally.

To make an alias permanent on user level edit **~/.bashrc** file.

In Linux world on command prompt any file or folder deleted once would be deleted forever. But we can make TRASH folder using alias command.

Make a **trash** folder. Keep it hidden. [Put a DOT in front of folder name]

```
$mkdir .trash
```

```
[user1@server ~]$ mkdir .trash
[user1@server ~]$ _
```

Open **.bashrc** file

```
[user1@server ~]$ vi .bashrc
```

In the end of file add following command

```
alias rm="mv -t ~/.trash"
```

rm command used to delete file or folder [with switch]

~ In Linux ~ (tilde sign) represent users home directory

```
# .bashrc
#
# Source global definitions
if [ -f /etc/bashrc ]; then
    . /etc/bashrc
fi

# User specific aliases and functions
alias rm="mv -t ~/.trash" ←
```

.bashrc file initialized when user login.

Logout from current session

```
[user1@server ~]$ exit_
```

login back

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: vimal
Password:
Last login: Tue Apr 28 11:59:24 on tty3
[vimal@server86 ~]$ alias
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias l='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias vi='vim'
alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot --show-tilde'
[vimal@server86 ~]$
```

Now when a user run **rm** command shell will actually execute **mv** command. Create a test file and delete it with **rm** command

```
[user1@server ~]$ cat > test_file
This file contain important information
What if you delete this file accidentally
Once deleted you can not restore it
Linux have no recycle bin
In Linux world once deleted delete forever
But we can custom recycle bin with help of alias command
[user1@server ~]$ rm test_file
[user1@server ~]$ ls
custom_script  Documents  Music      Public      tmp
Desktop        Downloads  Pictures   Templates  Videos
[user1@server ~]$ _
```

you can restore deleted file from trash folder. Restore our deleted file

```
[user1@server ~]$ cd .trash
[user1@server .trash]$ ls
test_file
[user1@server .trash]$ mv test_file ~
[user1@server .trash]$ cd
[user1@server ~]$ ls
custom_script Documents Music Public test_file Videos
Desktop Downloads Pictures Templates tmp
[user1@server ~]$ cat test_file
This file contain important information
What if you delete this file accidentally
Once deleted you can not restore it
Linux have no recycle bin
In Linux world once deleted delete forever
But we can custom recycle bin with help of alias command
[user1@server ~]$ _
```

To make an alias permanent on system level login from root and open **/etc/bashrc**

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64

server86 login: root
Password:
Last login: Tue Apr 28 12:05:57 on tty3
[root@server86 ~]# vim /etc/bashrc _
```

add your custom alias at the bottom of file and save it

```
unset i
unset pathmunge
fi
# vim:ts=4:sw=4

# System level custom alias
alias ls="ls -l" 
:wq_
```

logout from current session login back and test alias

```
Red Hat Enterprise Linux Server 7.0 (Maipo)
Kernel 3.10.0-123.el7.x86_64 on an x86_64
```

```
server86 login: root
Password:
Last login: Tue Apr 28 11:58:19 on tty3
[root@server86 ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg
[root@server86 ~]# _
```

How to unset alias

If you need new alias with same name than best way to remove an alias is by use the alias command to create a new alias with the same name. This overwrites the existing alias with that name.

If you only want to remove alias use **unalias** command

```
[user1@server ~]$ alias
alias .='ls -d .* --color=auto'
alias list='ls -l'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias rm='mv -t ~/trash'
alias vi='vim'
alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot --show-ti
lde'
[user1@server ~]$ unalias rm
[user1@server ~]$ alias
alias .='ls -d .* --color=auto'
alias list='ls -l'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias vi='vim'
alias which='alias | /usr/bin/which --tty-only --read-alias --show-dot --show-ti
lde'
[user1@server ~]$ _
```

If you have created permanent alias than open that file again and remove alias entry from configuration file.

```
unset i
unset pathmunge
fi
# vim:ts=4:sw=4
:wq_
```

We have created a system level alias [/etc/bashrc] in above example. To remove it we also need to remove its entry from file

Use of Linux alias command for system administrator

alias command can be used in several ways. Most popular use of alias command among the Linux system administrators are following

Use alias command to reduce the amount of typing

For example you frequently need to go in directory which have long path. You can create an alias for that directory and use it. Like we have a directory with the path

```
~/custom_script/linux/web_script/php/new_script
```

we can create an alias for it

```
$ alias new_php_script="cd ~/custom_script/linux/web_script/php/new_script"
```

Now whenever we need to go in that directory, we only need to type new_php_script on command prompt

```
$new_php_script
```

Use alias command to specify default options for command.

Like we have specified for ls command in above

Use alias command to create trash on command prompt

As we create in above example

Use alias command for safety of the system

A system administrator use alias to increase the safety of the system by making commands interactive. This forces the user to confirm that it is desired to perform a specific action and thereby reduces the risk from accidental or impulsive abuse of powerful commands.

For example **cp** command which is used to copy the contents of one file to another file, can also be reduced by making it interactive by default. If the name for the file to be written to does not exist in the specified directory (by default the current directory), it will be created, but if it already exists, its contents will be overwritten.

```
$alias cp="cp -i"
```

Above alias will reduce the chances of an unintended overwriting. Now if it detects any existing file with same name rather than overwriting that file shell would ask for confirmation.

Use alias to correct misspellings of commands.

For example a user which switched from window platform, he has a habit of typing **dir** instead of **ls**. We can create an alias for it in following way

```
$alias dir="ls"
```

Now user can use **dir** also to list the content.

sort command in linux

sort command allow you to sort the content of file. With sort command you can sort the contents in several ways. By default, the sort command sorts the contents in alphabetical order depending on the first letter in each line.

In this article we would cover following topic

Example of sort command

How to sort a file in alphabetical order in linux

How to sort by column in linux

How to sort in reverse order in linux

How to merge files with sort

How to sort files by size

List of options used with sort command

Example of sort command

Create a sample file with dummy names and age

```
$cat > test_file
```

```
[user1@server ~]$ cat > test_file
Sanjay, 30
Sarvan, 32
Vikarm, 12
Lussy, 27
Jon, 35
Vinita, 21
Maria, 25
Daya, 23
Albert, 19
[user1@server ~]$ _
```

How to sort a file in alphabetical order in linux

To sort this file alphabetically depending on name run following command

```
$sort test_file

[user1@server ~]$ cat > test_file
Sanjay, 30
Sarvan, 32
Vikarm, 12
Lussy, 27
Jon, 35
Vinita, 21
Maria, 25
Daya, 23
Albert, 19
[user1@server ~]$ sort test_file
Albert, 19
Daya, 23
Jon, 35
Lussy, 27
Maria, 25
Sanjay, 30
Sarvan, 32
Vikarm, 12
Vinita, 21
[user1@server ~]$ _
```

How to sort by column in linux

To sort this file depending on age run following command

```
$sort -k2 test_file
```

-k2 is the option which refers to the second column. You can specify other column also. Suppose that file contain 8 columns and your desired column number is 6 than you should use -k6.

```
[user1@server ~]$ sort test_file
Albert, 19
Daya, 23
Jon, 35
Lussy, 27
Maria, 25
Sanjay, 30
Sarvan, 32
Vikarm, 12
Vinita, 21
[user1@server ~]$ sort -k2 test_file
Vikarm, 12
Albert, 19
Vinita, 21
Daya, 23
Maria, 25
Lussy, 27
Sanjay, 30
Sarvan, 32
Jon, 35
[user1@server ~]$ _
```

How to sort in reverse order in linux

To sort in reverse order use -r option with sort command. You can also combine it with other options. To sort in reverse order of second column run following command

```
$sort -r -k2 test_file
```

```
[user1@server ~]$ sort -r -k2 test_file
Jan,      35
Jan,      35
Lussy,    34
Sarvan,   32
Sanjay,   30
Sanjay,   30
Lussy,    27
Maria,    25
Daya,     23
Vinita,   21
Vinita,   21
Albert,   19
Vikarm,   12
[user1@server ~]$ _
```

How to merge files with sort

```
[user1@server ~]$ cat test_file
Sanjay, 30
Sarvan, 32
Vikarm, 12
Lussy,  27
Jon,    35
Vinita, 21
Maria,  25
Daya,   23
Albert, 19
[user1@server ~]$ cat sample_file
Sodi,   45
Uakar,  34
Sachin, 35
Rani,   34
[user1@server ~]$ _
```

-m option allows us merge files in a single file.

```
[user1@server ~]$ sort -m sample_file test_file
Sanjay, 30
Sarvan, 32
Sodi,   45
Uakar,  34
Sachin, 35
Rani,   34
Vikarm, 12
Lussy,  27
Jon,    35
Vinita, 21
Maria,  25
Daya,   23
Albert, 19
[user1@server ~]$ _
```

How to save sort output in file

By default sort command will print out on standard output. Nothing is going to write in file. To save output in file either use -o option or use redirect.

```
[user1@server ~]$ cat demo_file
Sanjay, 30
Sarvan, 32
Sodi, 45
Uakar, 34
Sachin, 35
Rani, 34
Vikarm, 12
Lussy, 27
Jon, 35
Vinita, 21
Maria, 25
Daya, 23
Albert, 19
[user1@server ~]$ _
```

Use redirect method to save the output of sort command

```
[user1@server ~]$ sort -r demo_file > new_file
[user1@server ~]$ cat new_file
Vinita, 21
Vikarm, 12
Uakar, 34
Sodi, 45
Sarvan, 32
Sanjay, 30
Sachin, 35
Rani, 34
Maria, 25
Lussy, 27
Jon, 35
Daya, 23
Albert, 19
[user1@server ~]$ _
```

Use -o option to save the output of sort command in file

```
[user1@server ~]$ sort -r demo_file -o new_file1
[user1@server ~]$ cat new_file1
Vinita, 21
Vikarm, 12
Uakar, 34
Sodi, 45
Sarvan, 32
Sanjay, 30
Sachin, 35
Rani, 34
Maria, 25
Lussy, 27
Jon, 35
Daya, 23
Albert, 19
[user1@server ~]$ _
```

How to sort number in linux

Use -n option to sort based on number. Create a simple file with numbers and use default sort order.

It is sorted alphabetically.

```
[user1@server ~]$ cat > number_file
5
56
7
4
6
78
34
12
567
[user1@server ~]$ sort number_file
12
34
4
5
56
567
6
7
78
[user1@server ~]$ _
```

To sort this based on number use -n option

```
[user1@server ~]$ sort -n number_file
4
5
6
7
12
34
56
78
567
[user1@server ~]$ _
```

How to sort files by size

You can sort files by size with use of sort command. ls command is used to list the contents of directory.

```
[user1@server ~]$ ls -l
total 37
drwxrwxr-x. 2 user1 user1 1024 Sep 12 11:23 archived_file
-rw-rw-r--. 1 user1 user1 34 Sep 12 15:23 blank_space
drwxrwxr-x. 2 user1 user1 1024 Sep 12 11:52 cast_script
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Desktop
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Documents
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Downloads
-rw-rw-r--. 1 user1 user1 1024 Sep 12 13:57 example.tar
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Music
-rw-rw-r--. 1 user1 user1 24 Sep 12 15:10 number_file
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Pictures
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Public
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Templates
-rw-rw-r--. 1 user1 user1 134 Sep 12 15:35 test_file
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Videos
[user1@server ~]$ _
```

Use sort command with ls command to sort the files by size. As you can see in above image that size have column no 5. To sort the output of ls command based on size run following command

```
$sort ls -l | sort -k5
```

```
[user1@server ~]$ ls -l | sort -k5
total 37
-rw-rw-r--. 1 user1 user1 10240 Sep 12 13:57 example.tar
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Desktop
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Documents
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Downloads
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Music
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Pictures
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Public
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Templates
drwxr-xr-x. 2 user1 user1 1024 Sep 12 04:35 Videos
drwxrwxr-x. 2 user1 user1 1024 Sep 12 11:23 archived_file
drwxrwxr-x. 2 user1 user1 1024 Sep 12 11:52 cust_script
-rw-rw-r--. 1 user1 user1 134 Sep 12 15:35 test_file
-rw-rw-r--. 1 user1 user1 24 Sep 12 15:10 number_file
-rw-rw-r--. 1 user1 user1 34 Sep 12 15:23 blank_space
[user1@server ~]$ _
```

List of options used with sort command

- r Sorts in reverse order
- s Stabilize sort by disabling last-resort comparison
- t Use SEP instead of non-blank to blank transition
- u If line is duplicated only display once
- b Ignores blank spaces at beginning of the line.
- c Check whether input is sorted or not.
- d Use dictionary sort order and ignores the punctuation.
- f Ignores caps
- k Start a key at POS1, end it at POS2 (origin 1)
- m Merges two or more input files into one file.
- M Treats the first three letters in the line as a month (such as jun.)
- n Sorts by the beginning of the number at the beginning of the line.
- o Write result to FILE instead of standard output
- o outfile** Save the sorted output to a file.

We have listed most frequently options used with sort command. To get a full list of all options with details read man page of sort command

```
$man sort
```

How to find files in linux

In Linux world everything is file. Linux system is managed through the several configuration files. Most of configuration files have associated documentation file or sample file. You can use sample files in exam. For RHCE exam you should be able to find the file. It is very common to forget the path of file during the exam. You may know the name of file but not path in that case use these commands to find the file.

find

locate

find

find command need two arguments file name and location. Syntax of find command is

```
#find [location] -name [file name ]
```

find :- command

location :- where you want to search the file

-name :- option to specify the file name

file name :- name of file which you want to search

For example to search **vsftpd.conf** [FTP configuration file] file we would use following command

```
#find / -name vsftpd.conf
```

This would start search from top level root directory and list the found.

```
[root@server ~]# find / -name vsftpd.conf
/etc/vsftpd/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_USERS/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/INTERNET_SITE_NOINETD/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/INTERNET_SITE/vsftpd.conf
[root@server ~]#
```

Searching from root directory should be your last resources. When you perform search form root directory **find** command scan the entire Linux system for the desired file. It is time consuming process. Use subdirectories whenever you know it. For example if we know that vsftpd.conf file is located in **/etc** directory we should use following command

```
#find /etc -name vsftpd.conf
```

```
[root@server ~]# find / -name vsftpd.conf
/etc/vsftpd/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_USERS/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/INTERNET_SITE_NOINETD/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/INTERNET_SITE/vsftpd.conf
[root@server ~]# find /etc -name vsftpd.conf
/etc/vsftpd/vsftpd.conf
[root@server ~]# _
```

find command accepts wildcard. Wildcard allows us to find a file even we know only few characters of file name. For example our desired file starts from **vs** and have **.conf** in the end but we do not know the middle characters. In this case we would find it in following way

```
#find /etc -name vs*.conf
```

```
[root@server ~]# find /etc -name vsftpd.conf
/etc/vsftpd/vsftpd.conf
[root@server ~]# find /etc -name vs*.conf
/etc/vsftpd/vsftpd.conf
[root@server ~]# _
```

Wildcards

- * Any number of alphanumeric characters
- ? Single alphanumeric characters

Example of wildcards

Create a directory and move in it

```
[root@server ~]# mkdir practice_of_find
[root@server ~]# cd practice_of_find/
[root@server practice_of_find]# _
```

Make some blank files for practice of **find** command. Use **touch** command to create files.

```
[root@server practice_of_find]# touch file1.conf
[root@server practice_of_find]# touch demo.conf
[root@server practice_of_find]# touch DeMo.conf
[root@server practice_of_find]# touch deMo.conf
[root@server practice_of_find]# touch fileK.conf
[root@server practice_of_find]# touch 234
[root@server practice_of_find]# _
```

Find the files those start from **f** and end with **.conf**

It would returns with following error

find: paths must precede expression

```
[root@server practice_of_find]# find /root/practice_of_find -name f*.conf
find: paths must precede expression: fileK.conf
Usage: find [-H] [-L] [-P] [-Olevel] [-D help|tree|search|stats|rates|stop|exec] [
path...] [expression]
[root@server practice_of_find]# _
```

find command expand the wild card while it parse. So if result contain single match it would return without any error. Like in above example we searched for **vs*.conf** and it returned with correct result. But if result contains more than one match it would return with **find: paths must precede expression** error. It is because what find parsing in this case will look like

```
#find /root/practices_of_find -name file1.conf filek.conf
```

how to solve find: paths must precede expression error

solution of **find: paths must precede expression** error is very simple. Put the file name in quotes. It would stop the shell (bash) expanding your wildcards.

```
[root@server practice_of_find]# find /root/practice_of_find -name "f*.conf"
/root/practice_of_find/file1.conf
/root/practice_of_find/fileK.conf
[root@server practice_of_find]# _
```

Find the files which

have **file** in staring

later one character could be anything

ends with **.conf**

```
[root@server practice_of_find]# find /root/practice_of_find -name "file?.conf"
/root/practice_of_find/file1.conf
/root/practice_of_find/fileK.conf
[root@server practice_of_find]# _
```

locate

find command is too time consuming specially in 2 hour RHCE exam. use **locate** command instead of **find** in exam. **locate** command use a database of installed files and directories. **locate** command database updated only once in a day.

Syntax of **locate** command is following

```
#locate [file name]
```

locate command search form its database so it does not require path.

```
[root@server practice_of_find]# locate vsftpd.conf
/etc/vsftpd/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/INTERNET_SITE/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/INTERNET_SITE_NOINETD/vsftpd.conf
/usr/share/doc/vsftpd-2.2.2/EXAMPLE/VIRTUAL_USERS/vsftpd.conf
/usr/share/man/man5/vsftpd.conf.5.gz
[root@server practice_of_find]# _
```

Major drawback of **locate** command is that it update its database only once in a day. For example you can find **demo.conf** which we created in above example from **find** command but not from **locate** command.

database of **locate** command is updated from **/etc/cron.daily/mlocate.cron** script. We can manually run this script.

```
[root@server practice_of_find]# find /root/practice_of_find -name demo.conf
/root/practice_of_find/demo.conf
[root@server practice_of_find]# locate demo.conf
[root@server practice_of_find]# /etc/cron.daily/mlocate.cron
[root@server practice_of_find]# _
```

Now we can find **demo.conf** also from **locate** command

```
[root@server practice_of_find]# find /root/practice_of_find -name demo.conf
/root/practice_of_find/demo.conf
[root@server practice_of_find]# locate demo.conf
[root@server practice_of_find]# /etc/cron.daily/mlocate.cron
[root@server practice_of_find]# locate demo.conf
/root/practice_of_find/demo.conf
[root@server practice_of_find]# _
```

In exam

Update **locate** command database as soon as possible and use **locate** command whenever you need to search any file.

Use **find** command when **locate** does not works. Try to specify as much path as you remember when using **find** command.

how to find difference between two files in linux

diff command find the difference between files. In this article we would see how **diff** command can help us in RHCE exam.

Everything in Linux is managed through the several configuration files. During the exam you need to change the setting in several configuration files. You should always take backup before making any change in configuration file during the exam.

You can easily find out the changes which you have made if you have backup copy of configuration file.

Example of diff

We would modify **vsftpd.conf** file for practice.

ftp use **vsftpd.conf** configuration file for its setting. RHCE exam objective include ftp so you may have to configure it during the exam.

Create a directory and take backup of **vsftpd.conf** file

```
[root@server ~]# mkdir backup
[root@server ~]# cp /etc/vsftpd/vsftpd.conf /root/backup/
[root@server ~]# ls backup/
vsftpd.conf
[root@server ~]# _
```

Start the ftp service

```
[root@server ~]# chkconfig --list vsftpd
vsftpd           0:off  1:off  2:off  3:off  4:off  5:off  6:off
[root@server ~]# service vsftpd start
Starting vsftpd for vsftpd:                                         [ OK ]
[root@server ~]# service vsftpd status
vsftpd (pid 16245) is running...
[root@server ~]# _
```

ftp by default allow anonymous login. Open **vsftpd.conf**

```
[root@server ~]# chkconfig --list vsftpd
vsftpd           0:off  1:off  2:off  3:off  4:off  5:off  6:off
[root@server ~]# service vsftpd start
Starting vsftpd for vsftpd:                                         [ OK ]
[root@server ~]# service vsftpd status
vsftpd (pid 16245) is running...
[root@server ~]# vi /etc/vsftpd/vsftpd.conf _
```

Your task is to disallow anonymous login.

```
## Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid.
# loosens things up a bit, to make the ftp daemon more
# Please see vsftpd.conf.5 for all compiled in defaults
#
# READ THIS: This example file is NOT an exhaustive list
# Please read the vsftpd.conf.5 manual page to get a full
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if
# anonymous_enable=YES)                                     Setting for anonymous login
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command
write_enable=YES
#
# Default umask for local users is 077. You may wish to
# if your users expect that (022 is used by most other
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload
"/etc/vsftpd/vsftpd.conf" 118L, 4494C
```

Change configuration setting so ftp disable anonymous login and save the file

```

# The default compiled in settings are fairly paranoid. This
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of
# Please read the vsftpd.conf.5 manual page to get a full
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you
#anonymous_enable=YES <---- We only need to comment this line
sdf <---- This is wrong entry it would generate error
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change
# if your users expect that (022 is used by most other ftp
local_umask=022
#
"/etc/vsftpd/vsftpd.conf" 119L, 4499C written
[root@server ~]# _
```

Notice that I made a wrong setting. It would stop vsftpd service. Try to restart vsftpd service.

```

[root@server ~]# service vsftpd restart
Shutting down vsftpd: [ OK ]
Starting vsftpd for vsftpd: 500 OOPS: missing value in config file for: sdf
[FAILED]
[root@server ~]# _
```

vsftpd service failed with error. To troubleshoot this we need to check what settings we did in configuration file. Here comes the magic of **diff** command. With **diff** command we can easily find the modified settings.

```

[root@server ~]# service vsftpd restart
Shutting down vsftpd: [ OK ]
Starting vsftpd for vsftpd: 500 OOPS: missing value in config file for: sdf
[FAILED]
[root@server ~]# diff /root/backup/vsftpd.conf /etc/vsftpd/vsftpd.conf
12c12,13
< anonymous_enable=YES <---- Original file
-->
> #anonymous_enable=YES <---- Modified file
> sdf.
[root@server ~]# _
```

Line no. 12 modified
c for change

Line no 13
new added

Now we know the modified settings. **diff** command also tells us the line number of modified settings.

Open vsftpd.conf file again

```
[root@server ~]# vi /etc/vsftpd/vsftpd.conf
```

Display line number (To display line number use ESC + : + set nu)

```
# Default umask for local users is 077
# if your users expect that (022 is used)
local_umask=022
#
:set nu_ → Display line number
```

To fix the issue delete line no 13 [contain text sdf] and save the file.

```
1 # Example config file /etc/vsftpd/vsftpd.conf
2 #
3 # The default compiled in settings are fairly
4 # loosens things up a bit, to make the ftp da
5 # Please see vsftpd.conf.5 for all compiled
6 #
7 # READ THIS: This example file is NOT an exha
ns.
8 # Please read the vsftpd.conf.5 manual page
's
9 # capabilities.
10 #
11 # Allow anonymous FTP? (Beware - allowed by
out).
12 #anonymous_enable=YES → Modified line
13 sdf → New added line
14 # Delete this line and it would resolve the error
15 # Uncomment this to allow local users to log
16 local_enable=YES
17 #
18 # Uncomment this to enable any form of FTP wr
19 write_enable=YES
20 #

:set nu
```

Now restart the vsftpd service again.

```
[root@server ~]# service vsftpd restart
Shutting down vsftpd: [FAILED]
Starting vsftpd for vsftpd: [ OK ]
[root@server ~]#
```

Restore the original configuration file back after doing this practice.

```
[root@server ~]# cp /root/backup/vsftpd.conf /etc/vsftpd/vsftpd.conf
cp: overwrite '/etc/vsftpd/vsftpd.conf'? y
[root@server ~]#
```

How to get help for commands

You can use command help options to get more details. During the RHCE exam no internet access is available. But you can use local resources available in RHEL. During the exam whenever you have doubt about the options used with command take help.

Command itself

Run command itself without supplying any required options or arguments. For example we do not know the correct syntax of **grep** command. In this case we should run **grep** command by itself. It would give us hint about the correct syntax of **grep** command.

```
[root@server ~]# grep
Usage: grep [OPTION]... PATTERN [FILE]...
Try 'grep --help' for more information.
[root@server ~]# _
```

--help option

Running command by itself does not work for several commands. Like running **cp** command would not give us any information about command syntax or options.

```
[root@server ~]# cp
cp: missing file operand
Try 'cp --help' for more information.
[root@server ~]# _
```

Use **--help** option with command to get available help.

```
[root@server ~]# cp
cp: missing file operand
Try 'cp --help' for more information.
[root@server ~]# cp --help
```

info

Most of commands in RHEL have info manual. You should take help from info manual whenever it is available. info manual gives you detail about the associated options with short description. Syntax for **info** command is

```
#info [command]
```

```
[root@server ~]# info cp
```

man command

--help option list only most frequently used options. To list all available options with their details use man page. Linux commands are documented in a format known as the man page. **man** command list the options and settings associated with command. To use **man** command use following syntax

```
$man [command]
```

For example to get help about **ls** command

```
$man ls
```

```
[root@server ~]# man ls
```

During the exam sometime you may need help about any service or configuration value but do not know which man page is associated with that service. In such a situation use you can use **whatis** and **apropos** command. For example we want to know information about ntfs but do not know which man page has documentation about ntfs. Run **apropos** command to list all man pages which have ntfs in their description.

```
#apropos ntfs
```

```
[root@server ~]# apropos ntfs
smbcquotas          (1) - Set or get QUOTAs of NTFS 5 shares
vfs_acl_tdb          (8) - Save NTFS-ACLs in a tdb file
vfs_acl_xattr        (8) - Save NTFS-ACLs in Extended Attributes (EAs)
[root@server ~]# _
```

In same way to list all man page which has **ls** in their title run following command

```
#whatis ls
```

```
[root@server ~]# whatis ls
ls                  (1) - list directory contents
ls                  (1p) - list directory contents
[root@server ~]# _
```

Difference between **whatis** and **apropos** is that **whatis** look in title of man page while **apropos** search in description.

During the exam

Both **whatis** and **apropos** command depends on a database in the **/var/cache/man** directory. So if you have installed any RPM during the exam these commands would not be for that. Fortunately you can update the database at any time by running following command

```
# /etc/cron.daily/makewhatis.cron
```

Documentation directory

Path of documentation directory is **/usr/share/doc**. Documentation directory may include sample configuration files. So it is a better idea to check them as well. For example **sudo-*/** directory contain following sample configuration files.

sample.syslog.conf

sample.pam

sample.sudoers

```
[root@server ~]# cd /usr/share/doc/
[root@server doc]# ls sudo*
ChangeLog README           sample.syslog.conf      sudoers2ldif
HISTORY README.LDAP        schema.ActiveDirectory TROUBLESHOOTING
LICENSE  sample.pam         schema.iPlanet       UPGRADE
NEWS     sample.sudoers    schema.OpenLDAP
[root@server doc]# _
```

Grep & Pattern Matching

Grep is an acronym of Global Regular Expression Print. grep command required file or files name and pattern to search. It scans given file or files line by line and return the lines that contain the specified pattern.

This article enhances your knowledge on grep command which you have acquired from last article.

A regular expression is a way of specifying a pattern in text that can be applied to variable inputs to find all occurrences that match the pattern. A pattern is a sequence of characters.

Create a simple file and put some dummy data in it

```
[root@server ~]# cat example_file
This is a dummy file.
Sanjay software engineer $4000
Vinita network administrator $5000
Lussy content writer $2000
Vickey Desktop support $1000
jon software engineer $3000
above line contain name job and salary
this line contain special character %
our main software engineer is sanjay
vinita & vickey works in network department
[root@server ~]# grep sanjay$ example_file
our main software engineer is sanjay
[root@server ~]# _
```

how to find text string from grep command

RHCSA exam checks candidate's caliber to find text string from configuration or logs files. Beside exam as a Linux administrator you should know how to use grep to analyze text. In this article I am going to show how to find text string from files in rhel6.

how to find text string

grep returns any lines that have characters, words, or expressions that match your query. we could use grep in two ways either independent or with any commands.

- To use grep independent run grep with -r switch.
- To use grep with other command use | pipe sign.

In Linux system configuration and log files could contain several thousand lines.

For example we would like to find whether sshd service start on boot time or not, we would find sshd service status in /var/log/boot.log

```
[root@server ~]# grep -r sshd /var/log/boot.log
Starting sshd:
[root@server ~]# cat /var/log/boot.log | grep sshd
Starting sshd:
[root@server ~]# _
```



Take an another example, you would like to find the running process id of firefox use grep with ps command

```
[root@server ~]# ps -ef | grep firefox
root      2082  1896  0 03:22 ttys000  00:00:00 grep firefox
[root@server ~]# _
```

Now find in regular text file, first create a test file and then find any string from file

```
[root@server ~]# cat > test_file
This is line one
This is second line
This is third line
This is fourth line
This is fifth line
[root@server ~]# grep -r third test_file
This is third line
[root@server ~]# cat test_file | grep third
This is third line
[root@server ~]# _
```

Finally find in configuration file, check whether userlist_enable (a configuration value which check the access) is enable or not

```
[root@server ~]# grep -r userlist_enable /etc/vsftpd/vsftpd.conf
userlist_enable=YES
[root@server ~]# _
```

Case insensitive grep search

search for sanjay

```
[root@server ~]# grep -r sanjay example_file
our main software engineer is sanjay
[root@server ~]# _
```

Default grep command search is case sensitive. To make case insensitive search use -i option

```
[root@server ~]# grep -r sanjay example_file
our main software engineer is sanjay
[root@server ~]# grep -i -r sanjay example_file
Sanjay software engineer $4000
our main software engineer is sanjay
[root@server ~]# _
```

grep for words beginning and ending with

- Use ^ to match only at the start of line.
- Use \$ to match only at the end of line.

grep begins with

grep with ^ anchor would return all the line that start from given pattern. To match exacts word use -w option

```
[root@server ~]# cat > dummy_name
Sanjay
sanjay
sAnJay
sanjaykumar
SaNjAy
sanJay
[root@server ~]# grep ^sanjay dummy_name
sanjay
sanjaykumar
[root@server ~]# grep -w ^sanjay dummy_name
sanjay
[root@server ~]# _
```

grep ends with

```
[root@server ~]# cat example_file
This is a dummy file.
Sanjay software engineer $4000
Vinita network administrator $5000
Lussy content writer $2000 ^ Returns the line
Vickey Desktop support $1000 starting with
Jon software engineer $3000
above line contain name job and salary
this line contain special character %
our main software engineer is sanjay
Vinita & Vickey works in network department
[root@server ~]# grep ^Sanjay example_file
Sanjay software engineer $4000
[root@server ~]# grep sanjay$ example_file
our main software engineer is sanjay
[root@server ~]# _
$ Returns the line end with
```

Example question:-

Find the users which use the bash shell.

```
[root@server ~]# grep bash$ /etc/passwd
root:x:0:0:root:/root:/bin/bash
amandabackup:x:33:6:Amanda user:/var/lib/amanda:/bin/bash
sanjay:x:500:501:sanjay kumar goswami:/home/sanjay:/bin/bash
user1:x:501:502::/home/user1:/bin/bash
user2:x:502:503::/home/user2:/bin/bash
[root@server ~]# _
```

-i option makes pattern to case insensitive. That is not useful when we want to make only certain characters case insensitive from word.

In this case we can use pattern search with **[]**. Pattern search allow us to use any combination. There are already several ready to use combination which are known as character class. Character class is not going to be test in RHCE exam so we are not including it here. Check our Linux study guide for character classes.

For example we want to search

Both s and S

Both j and J

Than we would specify them in following manner

[sS] for both s and S

[jJ] for both j and J

```
[root@server ~]# cat dummy_name
Sanjay
sanjay
sAnJay
sanjaykumar
SaNjAy
sanJay
[root@server ~]# grep '[sS]an[jJ]ay' dummy_name
Sanjay
sanjay
sanjaykumar
sanJay
Match both s and S
Match both j and J
[root@server ~]# grep -w '[sS]an[jJ]ay' dummy_name
Sanjay
sanjay
sanJay
[root@server ~]# _ -w option will make it exact search
```

pattern search allows us to use digit as well

```
[root@server ~]# cat dummy_name
Sanjay1
sanjay
sAnJay3
sanjaykumar
SaNjAy
sanJay8
[root@server ~]# grep -w '[sS]an[jJ]ay[0-9]' dummy_name
Sanjay1
sanJay8
[root@server ~]# _
```

Search for two digits

```
[root@server ~]# cat dummy_name
Sanjay1
sanjay
sAnJay3
sanjaykumar
SaNjAy
san4Jay8
[root@server ~]# grep -w '[sS]an[0-9][jJ]ay[0-9]' dummy_name
Sanjay1
san4Jay8
[root@server ~]# _
```

Match at least one letter

```
[root@server ~]# cat dummy_digit
123 3434
12321 3432
34er 563
dfgdf 3434
2344 RRT5
[root@server ~]# grep [a-zA-Z] dummy_digit
34er 563
dfgdf 3434
2344 RRT5
[root@server ~]# _
```

Match at least one digit

```
[root@server ~]# cat dummy_name
Sanjay1
sanjay
sAnJay3
sanjaykumar
SaNjAy
san4Jay8
[root@server ~]# grep [0-9] dummy_name
Sanjay1
sAnJay3
san4Jay8
[root@server ~]# _
```

Search for special character

Special characters need to be escaped. For example to find & we need to use it '\&'

```
[root@server ~]# cat example_file
This is a dummy file.
Sanjay software engineer $4000
Vinita network administrator $5000
Lussy content writer $2000
Vickey Desktop support $1000
jon software engineer $3000
above line contain name job and salary
this line contain special character %
our main software engineer is sanjay
vinita & vickey works in network department
[root@server ~]# grep '\%' example_file
vinita & vickey works in network department
[root@server ~]# _
```

Example question:-

"/etc/hosts.allow" file contains the access rules for various network services. Check 192.168.1.23 has access or not.

```
[root@server ~]# cat /etc/hosts.allow
#
# hosts.allow    This file contains access rules which are used to
#                 allow or deny connections to network services that
#                 either use the tcp_wrappers library or that have been
#                 started through a tcp_wrappers-enabled xinetd.
#
#                 See 'man 5 hosts_options' and 'man 5 hosts_access'
#                 for information on rule syntax.
#                 See 'man tcpd' for information on tcp_wrappers
#
192.168.1.1
192.168.1.2
192.168.1.23

[root@server ~]# grep '192\.168\.1\.23' /etc/hosts.allow
192.168.1.23
[root@server ~]# _
```

egrep

With **grep** command meta characters [+, ?, |, (,)] loss their special meanings. For example + have a special meaning "one or more times" but if we use it with grep command it would return the line which contains +. To use meta characters with their special meanings use **egrep** [acronym of Extended Global Regular Expressions Print] command.

```
[root@server ~]# cat test
this is test file
second line ?
third + four
5 ( means five )
[root@server ~]# grep "+" test
third + four
[root@server ~]# egrep "+" test
this is test file
second line ?
third + four
5 ( means five )
[root@server ~]# _
```

fgrep

fgrep [acronym of "Fixed-string Global Regular Expressions Print"] does NOT recognize any regular expression meta-characters as being special. For example if we want to search the line which contains (.) DOT . For grep command dot is a meta character that means 'wild-card, any single character'.

```
[root@server ~]# cat > test
this file contains special characters ?
what if i need to search . in line
[root@server ~]# grep '.' test
this file contains special characters ?
what if i need to search . in line
[root@server ~]# fgrep '.' test
what if i need to search . in line
```

pgrep

pgrep (acronym of Process-ID Global Regular Expressions Print) scan the currently running processes and lists the process IDs which matches the provided selection criteria. For example, if I want to know the process ID of my sshd process

```
[root@server ~]# pgrep sshd
1418
[root@server ~]# _
```

This article is the part of our RHCE Study guide. It is a simplified version of grep command for the RHCE exam candidate. If you are a Linux administrator or need more details about grep command please check our Linux study guide.

USERADD

The useradd command creates a new user account. The new user account will be entered into the system files as below.

/etc/passwd
/etc/shadow
/etc/group
/etc/gshadow
/var/spool/mail
/home

Apply security to user's home directory

user add contain some user profile set directory and each directory contain some hidden files. these files are known as skeleton files.

location of skeleton file : /etc/skel/

/etc/passwd - when we create any new user, this file contain information about the newly added user. when we open this file there is some entries such as below.

Syntax : - #vim /etc/passwd

e.g. - Student:x:500:500::/home/Student:/bin/bash

each field have some meaning explain in below .

“Student” - this field represent the user name.

“x” - pointer or link to password to given user.

“500” - user id, each and every user have there own unique id. Range of UID is 0-65535 and Root user have 0 UID.

“500” - Group id, it also have range between 0-65535.

“: : “- This field is use to add some string with your name it is known as comment field. Actual name of this field is GECOS. GECOS can store multiple information about any user. This information is known as finger database.

Syntax :- finger <username>

Description :- show the detailed information about user.

Syntax :- chfn <username>

Description :- Above syntax is used for add or update details for the already existing user.

“/home/Student”:- location of user's home directory.

“/bin/bash” - path of shell for user.

Note:-

Administrator account in Linux is known as root account it have UID 0.
General account or shell account have UID between 500-60000.

System accounts and service accounts have UID between 1-499 & 60001-65535. These accounts are never logged-in but they provide some services for the user.

/etc/shadow - file stores actual password in encrypted format for user's account with additional properties related to user password.

Syntax :- #vim /etc/shadow

e.g. student:\$1\$Pluwi7C\$EsvYAfV4kgcPjYnR9iLVA1:15699:0:99999:7:::

“student” - It is your log in name.

“\$1\$Pluwi7C\$EsvYAfV4kgcPjYnR9iLVA1” - It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits. if it starts with “\$1\$” it means the MD5-based algorithm was used.

“15699” - Days since Jan 1, 1970 that password was last changed.

“0” - The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password.

“99999” - The maximum number of days the password is valid (after that user is forced to change his/her password).

“7” - The number of days before password is to expire that user is warned that his/her password must be changed.

“::” - The number of days after password expires that account is disabled.

“::” - days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the log in may no longer be used.

This field is reserved for future use.

/etc/group - file is world-readable and contains a list of groups, each on a separate line. Each line is a four field, colon delimited list including the following information.

Syntax:- #vim /etc/group

e.g. student:x:500:student,linuxworld, vimal

“student” - Group Name . Used by various utility programs as a human-readable identifier for the group.

“x” - *Group password* If set, this allows users that are not part of the group to join the group by using the newgrp command and typing the password stored here. If a lower case x is in this field, then shadow group passwords are being used.

“500” - *Group ID (GID)* The numerical equivalent of the group name. It is used by the operating system and applications when determining access privileges.

Last field is use to *Member list*, A comma delimited list of the users belonging to the group.

/etc/gshadow - This file is readable only by the root user and contains an encrypted password for each group, as well as group membership and administrator information.

Syntax: - #vim /etc/gshadow

e.g. student:!:vimal: student,linux world,vimal

“student” - The name of the group.

“!” - The encrypted password for the group. If set, non-members of the group can join the group by typing the password for that group using the newgrp command. If the value of this field is !, then no user is allowed to access the group using the newgrp command. A value of !! is treated the same as a value of ! — however, it also indicates that a password has never been set before. If the value is null, only group members can log into the group.

Syntax of set group password - #gpasswd <username>

Group Administrator listed here (in a comma delimited list) can add or remove group members using the gpasswd command.

Group members listed here (in a comma delimited list) are regular, non-administrative members of the group.

Some important Syntax:-

#useradd -G <user name> <Group name> “This syntax is use to add a user into already exiting group.”

#usermod -G <user name> <Group name> “This syntax is use to change group of existing user.

#userdel <user name> “This syntax is use to delete already exist user. It will delete only user. There home directory and mail directory will not deleted.”

#userdel -r <username> “This syntax is also work like as above but it will delete home directory and mail directory of selected user.”

#groupadd <group name> “This syntax is use to add a new group.”

5 Useradd Create a Directory of Supplied Username Under /home Directory

6 Useradd Implements Some Security In User’s Home Directory

7 Useradd Creates a Mailbox For Same User Inside /var/spool/mail

8 Useradd Copies Some Internal Files Inside Users Home Directory From /etc/Skel

Chmod permissions In linux

chmod command can be used to change different permission configurations. chmod takes two lists as its arguments: permission changes and filenames.

You can specify the list of permissions in two different ways. One way uses permission symbols and is referred to as the symbolic method. The other uses what is known as a “binary mask” and is referred to as either the absolute or the relative method.

Symbolic Method

The symbolic method of setting permissions uses the characters **r, w, and x** for read, write, and execute, respectively. Any of these permissions can be added or removed. The symbol to add a permission is the **plus sign, +**. The symbol to remove a permission is the **minus sign, -**.

chmod :- File Permissions in Symbolic Method

Description	
R	Read
W	Write
X	Execute (also gives permission to change into a directory)
X	Execute only if it is a directory or has execute permission for some user
S	Set user or group ID on execution
T	Sticky bit
U	Permissions granted to user who owns the file
G	Permissions granted to users in the file's group
O	Permissions granted to owner of the group and users in the file's group

r w x permissions

The first three (r, w, x) are clear. Use them to set read, write, and execute permissions.

s permission

The s permission is used on directories to keep the user or group ID for a file created in the directory. To set the user ID for any new files created in the directory to the owner of the directory, use the chmod u+s <directory> command. To set the group ID for any new files created in the directory to the directory's group, use the chmod g+s <directory> command.

t permission

t is a special permission which provides greater security on directories. Sticky bit is used for directories to protect files within them. Files in a directory with the sticky bit set can only be deleted or renamed by the root user or the owner of the directory.

u g o permission

The last three permissions (u, g, o) are only used with the = operator to set permissions for the owner, group, others, or everyone equal to the existing permissions for the owner, group, others, or everyone. For example, chmod g=u [filename] sets the group permissions to the current permissions for the owner of the file.

Examples of symbolic method

```
[root@localhost ~]# mkdir test
[root@localhost ~]# ls -ld test
drwxr-xr-x 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod u+rwx test
[root@localhost ~]# ls -ld test
drwxr-xr-x 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod g+rwx test
[root@localhost ~]# ls -ld test
drwxrwxr-x 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod o+rwx test
[root@localhost ~]# ls -ld test
drwxrwxrwx 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod o-rwx test
[root@localhost ~]# ls -ld test
drwxrwx--- 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod g-rwx test
[root@localhost ~]# ls -ld test
drwxr----- 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# _
```

Absolute Permissions: Binary Masks

The absolute method changes all the permissions at once, instead of specifying one or the other. It uses a binary mask that references all the permissions in each category.

Binary Masks

When dealing with a binary mask, you need to specify three digits for all three categories, as well as their permissions. This makes a binary mask less flexible than the permission symbols.

Digits	permission
0	none
1	execute
2	write
4	read
3 (1+2)	write and execute
5 (1+4)	read and execute
7 (1+2+4)	read write execute

Value	Meaning
777	(rwxrwxrwx) No restrictions on permissions. Anybody may do anything. Generally not a desirable setting.
755	(rwxr-xr-x) The file's owner may read, write, and execute the file. All others may read and execute the file. This setting is common for programs that are used by all users.
700	(rwx---) The file's owner may read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only the owner may use and must be kept private from others.
666	(rw-rw-rw-) All users may read and write the file.
644	(rw-r-r-) The owner may read and write a file, while all others may only read the file. A common setting for data files that everybody may read, but only the owner may change.
600	(rw----) The owner may read and write a file. All others have no rights. A common setting for data files that the owner wants to keep private.

Examples of binary masks

```
[root@localhost ~]# chmod 777 test
[root@localhost ~]# ls -ld test
drwxrwxrwx 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod 755 test
[root@localhost ~]# ls -ld test
drwxr-xr-x 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod 744 test
[root@localhost ~]# ls -ld test
drwxr--r-- 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod 700 test
[root@localhost ~]# ls -ld test
drwx----- 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# chmod 775 test
[root@localhost ~]# ls -ld test
drwxrwxr-x 2 root root 4096 Jan 23 03:01 test
[root@localhost ~]# _
```

Permission	Owner	Group	Other	
Read	x	x	x	
Write	x	x	x	777
Execute	x	x	x	

Permission	Owner	Group	Other	
Read	x	x	x	
Write	x			755
Execute	x	x	x	

Permission	Owner	Group	Other	
Read	x	x	x	
Write	x			744
Execute	x			

Permission	Owner	Group	Other	
Read	x			
Write	x			700
Execute	x			

Permission	Owner	Group	Other	
Read	x	x	x	
Write	x	x		775
Execute	x	x	x	

Permission	Owner	Group	Other
Read - 4	x	x	
Write - 2	x	x	x
Execute - 1	x	x	x
	$4 + 2 + 1 =$	$4 + 2 + 1 =$	$2 + 1 =$
	7	7	3

Defaults Permission : umask

Whenever you create a file or directory, it is given default permissions. You can display the current defaults or change them with the **umask** command. The permissions are displayed in binary or symbolic format. The default permissions include any execute permissions that are applied to a directory. Execute permission for a file is turned off by default when you create it because standard data files do not use the executable permissions (to make a file executable like a script, you have to manually set its execute permission). To display the current default permissions, use the **umask** command with no arguments.

The **-S** option uses the symbolic format.

```
#umask -S u=rwx,g=rx,o=rx
```

This default umask provides **rw-r--r--** permission for standard files and adds execute permission for directories, **rwxr-xr-x**.

You can set a new default by specifying permissions in either symbolic or binary format. To specify the new permissions, use the **-S** option. The following example denies others read permission, while allowing user and group read access, which results in permissions of **rwxr-x---**:

```
#umask -S u=rwx,g=rx,o=
```

When you use the binary format, the mask is the inverse of the permissions you want to set. To set both the read and execute permission on and the write permission off, you use the octal number 2, a binary 010. To set all permissions on, you use an octal 0, a binary 000.

The following example shows the mask for the permission defaults **rwx, rx, and rx** (rw, r, and r for files):

```
#umask 0022
```

When you use the octal number 2, the inverse of the permissions you want to set is 010. This means that the user has read and execute permission, while the group and others have only read permission. To set all permissions on, you use an octal 0, a binary 000.

```
#umask 0027
```

Change in umask from RHEL6

From RHEL6 no matter what the value of umask, new files can no longer be automatically created with executable permissions. For example, a umask value of 0454 leads to identical permissions on new files as a umask value of 0545. You need to use commands such as chmod to set executable permissions on a specific file.

Default value of umask is set in /etc/bashrc file.

Chmod Example

In our last article you learnt about permission. Permission can be set by chmod command in two different way symbolic and binary masks.

In this article we will practically implements whatever you have learnt so far in file permissions. This article is a sequential of last article if you have missed last article we suggest you to review them before going through this first.

Create 3 user a b c without password. Use for loop despite of creating them separately. You have learnt about this in our advance user managements assignments.

```
#for user in a b c
>do
>useradd $USER
>passwd -d $USER
>done
```

```
[root@localhost ~]# for USER in a b c
> do
> useradd $USER
> passwd -d $USER
> done
Removing password for user a.
passwd: Success
Removing password for user b.
passwd: Success
Removing password for user c.
passwd: Success
[root@localhost ~]# _
```

Now create a group example and add user a and b to it.

```
#groupadd example
#usermod -G example a
#usermod -G example b
```

```
[root@localhost ~]# groupadd example
[root@localhost ~]# usermod -G example a
[root@localhost ~]# usermod -G example b
[root@localhost ~]# _
```

now create a test directory on root partition and change ownership to user a and group to example.

```
[root@localhost ~]# mkdir /test
[root@localhost ~]# chown a /test
[root@localhost ~]# chgrp example /test
[root@localhost ~]# _
```

Now logon in 3 separate terminals form these users.

From root set permission to

```
#chmod 700 /test
```



```
[root@localhost ~]# chmod 700 /test
[root@localhost ~]# ls -ld /test
drwx----- 2 a example 4096 Jan 23 03:25 /test
[root@localhost ~]# _
```

This will set permissions to

```
owner a full
group example ( a ,b ) none
other c none
```

to verify these permission go on the terminals where user a is logged on and run following commands

```
$cd /test
$cat > a_file
This is a file of user a
$ls a_file
```

```
localhost login: a
[ a@localhost ~ ]$ cd /test
[ a@localhost test ]$ cat > a_file
this file is created by user a
[ a@localhost test ]$ ls
a_file
[ a@localhost test ]$ _
```

user a will be able to do all three task read write execute as owner have all three permission Now try to change /test directory form user b . It will deny. Because user b remain in example group. and group have no permissions.

```
localhost login: b
[ b@localhost ~ ]$ cd /test
-bash: cd: /test: Permission denied
[ b@localhost ~ ]$ _
```

Now try to change /test directory form user c. it will also deny. Because user c is other for this directory and other have no permissions.

```
localhost login: c
[ c@localhost ~ ]$ cd /test
-bash: cd: /test: Permission denied
[ c@localhost ~ ]$ _
```

Now change permission from root to

```
#chmod 710 /test
[root@localhost ~]# chmod 710 /test
[root@localhost ~]# ls -ld /test
drwx--x--- 2 a example 4096 Jan 23 03:25 /test
[root@localhost ~]# _
```

This will give full permission to owner a. And execute to b (b is in the group of a which is example) User c (other) still have no permissions.

To verify try change directoy form user b to /test it would be success but he will not be able to list the contain of directory.

```
$cd /test $ls
```

```
[b@localhost test]$ ls
a_file
[b@localhost test]$ cat > b_file
-bash: b_file: Permission denied
[b@localhost test]$ _
```

Also verify the permission of c (other) by changing the directory to /test

```
$cd /test
```

```
localhost login: c
[c@localhost ~]$ cd /test
-bash: cd: /test: Permission denied
[c@localhost ~]$ _
```

Now change permission from root to

```
#chmod 751 /test
```

```
[root@localhost ~]# chmod 751 /test
[root@localhost ~]# ls -ld /test
drwxr-x--x 2 a example 4096 Jan 23 03:25 /test
[root@localhost ~]# _
```

This will give full permission to owner a. execute and read to b (b is in the group of a which is example) User c (other) now have execute permissions.

To verify try to list form user b to /test it would be success but he will not be able to write in directory.

```
$ls $cat > b_file
```

```
[b@localhost test]$ ls
a_file
[b@localhost test]$ cat > b_file
-bash: b_file: Permission denied
[b@localhost test]$ _
```

Also verify the permission of c (other) by changing the directory to /test

```
$cd /test $ls
```

```
[c@localhost ~]$ cd /test
[c@localhost test]$ ls
ls: .: Permission denied
[c@localhost test]$ _
```

Now change permission from root to

```
#chmod 775 /test
```

```
[root@localhost ~]# chmod 775 /test
[root@localhost ~]# ls -ld /test
drwxrwxr-x 2 a example 4096 Jan 23 03:25 /test
[root@localhost ~]# _
```

This will give full permission to owner a b (b is in the group of a which is example) User c (other) now have read and execute permissions.

To verify try make new file form user b to /test it would be success.

```
$cd /test $ls $ cat > b_file This file is created by b
[b@localhost test]$ ls
a_file
[b@localhost test]$ cat > b_file
this is the file of b user
[b@localhost test]$ _
```

Also verify the permission of c (other) by listing the directory to /test

```
$cd /test $ls
[c@localhost test]$ ls
a_file b_file
[c@localhost test]$ cat > c_file
-bash: c_file: Permission denied
[c@localhost test]$ _
```

Now change permission from root to

```
#chmod 777 /test
```

```
[root@localhost ~]# chmod 777 /test
[root@localhost ~]# ls -ld /test
drwxrwxrwx 2 a example 4096 Jan 23 03:25 /test
[root@localhost ~]# _
```

This will give full permission to owner a b and c. User c (other) now have full permissions.

To verify make file form user c

```
$ cat > c_file This file is created by user c
[c@localhost test]$ ls
a_file b_file
[c@localhost test]$ cat > c_file
this file created by c user
[c@localhost test]$ _
```

how to set sticky bit

In our previous articles we have discussed about read write and execute permission for file and directory. Now I will show you some special permission which you can set for files and directories.

Sticky Bit Permissions

Sticky Bit is used for directories to protect files within them. Files in a directory with the sticky bit set can only be deleted or renamed by the root user or the owner of the directory.

Sticky Bit Permission Using Symbols

The sticky bit permission symbol is t. The sticky bit shows up as a t in the execute position of the other permissions. A program with read and execute permissions with the sticky bit has its permissions displayed as r-t.

```
# chmod +t /home/vinita/data
# ls -l /home/vinita/data -rwxr-xr-t 1 root root 4096 /home/vinita/data
```

Sticky Bit Permission Using the Binary Method

As with ownership, for sticky bit permissions, you add another octal number to the beginning of the octal digits. The octal digit for the sticky bit is 1 (001). The following example sets the sticky bit for the data directory:

```
# chmod 1755 /home/vinita/data
```

To remove sticky bit use minus sign.

```
#chmod o-t /example
[root@localhost ~]# chmod o-t /example
[root@localhost ~]# ls -ld /example
drwsrwsrwx 2 root root 4096 Jan 23 03:40 /example
[root@localhost ~]# _
```

now Vinita can delete the files owned by nikita verify

```
[vinita@localhost example]$ ls -l
total 8
-rw-rw-r-- 1 nikita root 6 Jan 23 03:36 nikita_file
-rw-rw-r-- 1 vinita root 5 Jan 23 03:36 vinita_file
[vinita@localhost example]$ rm nikita_file
rm: remove write-protected regular file 'nikita_file'? y
[vinita@localhost example]$ rm vinita_file
[vinita@localhost example]$ ls
[vinita@localhost example]$ _
```

how to set Sgid

This Permission is use to set any group automatically files / directory created by any member of group

```
# chgrp manager /home/vinita/data
```

Here manager is the name of group

To set sgid permission use below command

```
# chmod 2755 /home/vinita/data
```

File System Administration

In this section you would learn how to manage Linux file system. We would start from troubleshooting commands used in file system management. Later you would learn how to create partition from command prompt. We would include basic, LVM and raid partitions. In end of this section you would learn how to secure data with luks.

Useful commands to check file system status

In RHEL7 several commands are available for file system managements. In this article we would discuss only those commands which you may need in RHCE7 exams. Before you start practice of creating and deleting partition it is better to do some practice with these commands.

df

This is handy command to check available free space. Run **du** command

```
[root@server ~]# df
Filesystem      1K-blocks    Used   Available  Use% Mounted on
/dev/sda2        8063408  2363988   5289820  31% /
tmpfs            396264       100   396164   1% /dev/shm
/dev/sda1        198337   27019   161078  15% /boot
/dev/sda5        495844   10524   459720   3% /home
[root@server ~]#
```

If you feel difficulty in understanding the blocks use **-h** switch with **du** command

```
[root@server ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2        7.7G  2.3G  5.1G  31% /
tmpfs            387M  100K  387M   1% /dev/shm
/dev/sda1        194M   27M  158M  15% /boot
/dev/sda5        485M   11M  449M   3% /home
/dev/sr0          58M   58M     0  100% /media/VMware Tools
[root@server ~]#
```

Now outputs of **du** command look more users friendly. You could skip **tmpfs** and **/dev/sr0** as **tmpfs** stand for temporary space and **/dev/sr0** is my media device. This output is very useful when you need to manage disk. You could get an idea about which partition need more space or which partition has unused free space. Linux LVM gives you an ability to change partition size without losing any data. With LVM you could reduce the size of partition which has unnecessary free space or you could expand the size of partition which requires more space. **du** command is very helpful when you need to make such a decision. As output of this command show size of my root partition is 7.7G and currently I am using 2.3G and available free space is 5.1G which is fine. Currently none of my partition requires more space. During the practice of LVM we would use this more frequently.

du

This is useful command to check the size of file. While df commands show the available space in partitions, du commands show the size of files in partitions. you could use df command to check the space used by each partitions. if you need more detail about any specific partition like which file is consuming more space then you could use du command.

For example we would like to know

how much space is used by /boot partition?

how much space is available in /boot partition?

what is the size of each files and directories in /boot partition?

To get the answer of these questions we would first execute df command with -h switch. It would gives us the answer of first and second question. To know the answer of third question use du command with -h switch.

```
[root@server ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2        7.7G  2.4G  5.0G  32% /
tmpfs           387M  100K  387M   1% /dev/shm
/dev/sda1       194M   27M  158M  15% /boot
/dev/sda5       485M   11M  449M   3% /home
/dev/sr0          58M   58M     0 100% /media/VMware Tools
[root@server ~]# du -h /boot
13K  /boot/lost+found
245K  /boot/efi/EFI/redhat
247K  /boot/efi/EFI
249K  /boot/efi
276K  /boot/grub
21M   /boot
[root@server ~]#
```

You may get confuse from output. As df commands show boot partition is using 27 MB while du command is showing that /boot is using 21 MB so where is remaining 6 MB space?. This space is used by hidden files. You could use du command with -a switch to show the hidden files.

```
[root@server ~]# du -ha /boot_
```

mount

mount is the another helpful command. During the practice we would create and format partitions. mount command would show the file system type of partition. and it also help to know to the type of mount.

```
[root@server ~]# mount
/dev/sda2 on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 on /boot type ext4 (rw)
/dev/sda5 on /home type ext4 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
[root@server ~]#
```

fstab configuration file

In Linux everything is represented as files. During the boot process directories specified in /etc/fstab are mounted on configured volumes, with the help of the **mount** command. In exam you would create update and delete partition. To keep these changes after reboot we need to update fstab file. Linux normally automates mount the directory using the /etc/fstab configuration file during the boot process.

Any wrong entry in this file could crash the linux system. Before you start working with fstab file take backup first.

```
[root@server test]# cp /etc/fstab /etc/fstab.bk
[root@server test]# _
```

We suggest you to pay some time in understanding this file.



The diagram illustrates the structure of the /etc/fstab file with numbered callouts:

- 1 UUID DEVICE**: A green oval highlights the first line: `UUID=078a11a3-3070-43d5-b4a4-0ff99f184bc4 / ext4 defaults 0 0`.
- 2 MOUNT POINT**: A green rounded rectangle highlights the second line: `/dev/shm /dev/pts /sys /proc`.
- 3 FILESYSTEM FORMAT**: A green rounded rectangle highlights the third line: `tmpfs defaults gid=5,mode=620 0 0`.
- 4 MOUNT OPTION**: A green rounded rectangle highlights the fourth line: `defaults defaults 0 0`.
- 5 DUMP VALUE**: A green oval highlights the fifth line: `0 0`.
- 6 FILE SYSTEM CHECK ORDER**: A green oval highlights the sixth line: `0 0`.

```
#
# /etc/fstab
# Created by anaconda on Sat Aug 11 19:06:28 2012
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=078a11a3-3070-43d5-b4a4-0ff99f184bc4 / ext4 defaults 0 0
UUID=56f99ced-0da2-4244-9976-42f61212ceca /boot ext4 defaults 0 0
UUID=55a76f14-28b4-43eb-8d0a-4b216a246646 /home ext4 defaults 0 0
UUID=1a2769c8-a5ac-480d-8f21-1b8b99670392 swap swap defaults 0 0
tmpfs /dev/shm /dev/pts /sys /proc
tmpfs defaults gid=5,mode=620 0 0
defaults defaults 0 0
0 0
0 0
```

[/etc/fstab explain from left to right](#)

Sr.	Field Name	Description
-----	------------	-------------

1	Device	Label or UUID of device to be mounted
2	Mount Point	directory where the filesystem will be mounted
3	Filesystem Format	<p>Describes the filesystem type. Valid filesystem types are ext, ext2, ext3, ext4, msdos, vfat, devpts, proc, tmpfs, udf, iso9660, nfs, smb, and swap.</p> <ul style="list-style-type: none"> • The tmpfs filesystem is a virtual memory filesystem that uses both RAM and swap space. • The devpts filesystem relates to pseudo-terminal devices. • The sysfs filesystem provides dynamic information about system devices. • The proc filesystem is especially useful, as it provides dynamically. • ext3 is the default filesystem for RHEL 5. • ext4 is the default filesystem for RHEL 6. • Xfs is the default filesystem for RHEL7.
4	Mount Options	<p>Available mount points are exec, noatime, noauto, nodev, noexec, nosuid, nouser, remount, ro, rw, suid, sync, user.</p> <p>Use default in this field which contain following option default mount options rw, suid, dev, exec, auto, nouser, and async</p>
5	Dump Value	value for dump command. 1 means data is automatically save to disk when you exit Linux.
6	Filesystem Check Order	<p>check order for filesystems during the boot process.</p> <p>0 not checked during the boot process, default for CD/DVD</p> <p>1 checked on first place, default for root / system</p> <p>2 checked on second place, default for local filesystem like /home</p>

UUID

Short for Universally Unique Identifiers.

Every formatted volume has an UUID, a unique 128-bit number. Each UUID represents either a partition, a logical volume, or a RAID array. This is a new feature added from RHEL6. It is the same as RHEL5 LABEL option. UUID is automatically created when the volume is formatted with a command like mkfs.ext4.

fdisk utility

fdisk is available in all major operating systems including Microsoft Windows and Mac OS. But we would discuss only Linux version of fdisk. With fdisk utility you could create, update and delete partitions. In this article we would explore the fdisk command options. Later in this section we would use fdisk command to manage partitions.

Explore fdisk command options

How to check available switches of fdisk command

To check available switches with fdisk command run **fdisk** command without any switch

```
[root@server ~]# fdisk

Usage:
fdisk [options] <disk>      change partition table
fdisk [options] -l <disk>    list partition table(s)
fdisk -s <partition>        give partition size(s) in blocks

Options:
-b <size>                  sector size (512, 1024, 2048 or 4096)
-c                        switch off DOS-compatible mode
-h                        print help
-u <size>                  give sizes in sectors instead of cylinders
-v                        print version
-C <number>                specify the number of cylinders
-H <number>                specify the number of heads
-S <number>                specify the number of sectors per track

[root@server ~]# _
```

How to check available disk and partitions with fdisk command

To check available disk and partitions on file system use **-l** switch with **fdisk** command

```
[root@server ~]# fdisk -l

Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf

      Device Boot      Start        End      Blocks   Id  System
/dev/sda1  *           1         26     204800   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2            26        1046    8192000   83  Linux
/dev/sda3            1046       1177    1048576   82  Linux swap
/dev/sda4            1177       1567    3136512   5   Extended
/dev/sda5            1177       1241      512000   83  Linux
[root@server ~]# _
```

output show currently we have five partitions on **/dev/sda** disk. To manage disk with fdisk command we need to pass disk location as argument . Whenever you start working with fdisk command, **fdisk -l** command should be first on list. It would give you location of disk which is need by fdisk command.

Now we have mount point of disk so we could start fdisk command.

To start **fdisk** command pass mount point of disk as argument

```
[root@server ~]# fdisk /dev/sda
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help): _
```

as you could see in output you would get a warning message. Whether you made recommended change or not result would be same. In exam we should focus on result. So simple ignore it. Whether or not recommended changes are made, fdisk provides the same prompt, where you can press **m** to list basic fdisk commands.

press **m** on fdisk command prompt to get the list of all available commands

```
Command (m for help): m
Command action
  a  toggle a bootable flag
  b  edit bsd disklabel
  c  toggle the dos compatibility flag
  d  delete a partition
  l  list known partition types
  m  print this menu
  n  add a new partition
  o  create a new empty DOS partition table
  p  print the partition table
  q  quit without saving changes
  s  create a new empty Sun disklabel
  t  change a partition's system id
  u  change display/entry units
  v  verify the partition table
  w  write table to disk and exit
  x  extra functionality (experts only)

Command (m for help): _
```

During the exam never hesitate to take help. You should use all available resources. We use fdisk in next article so press **q** to quite form fdisk.

```
Command (m for help): q
[root@server ~]# _
```

how to create partition using fdisk

In this article we would use fdisk to create and manage partition. This article assumes that you have a new hard disk (or at least empty space on a current hard drive where you can add a new partition).

Create a new partition of 100 MB using fdisk, format it with ext4 filesystem, and configure it on the /test1 directory in /etc/fstab so that the new partition is properly mounted the next time you boot Linux.

As you have learnt from previous article **fdisk** command need hard disk mount point as argument. Check hard disk mount point

```
[root@server ~]# fdisk -l

Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf

      Device Boot   Start     End   Blocks   Id  System
/dev/sda1  *       1       26    204800   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2       26      1046   8192000   83  Linux
/dev/sda3      1046      1177   1048576   82  Linux swap
/dev/sda4      1177      1567   3136512    5  Extended
/dev/sda5      1177      1241   512000   83  Linux
[root@server ~]# _
```

Start **fdisk** command.

```
[root@server ~]# fdisk /dev/sda
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
```

At the fdisk command line prompt, start with the print command (**p**) to print the partition table. This allows you to review the current entries in the partition table. As discuss in previous article it is not necessary to switch off DOS mode. So it is up to you whether you want to follow the recommendations or not. If you want to follow the recommendations execute following command or if you want to ignore the recommendation skip this

```
Command (m for help): p
Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf

      Device Boot   Start     End   Blocks   Id  System
/dev/sda1  *       1      26    204800   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2        26     1046   8192000   83  Linux
/dev/sda3     1046     1177   1048576   82  Linux swap
/dev/sda4     1177     1567   3136512    5  Extended
/dev/sda5     1177     1241      512000   83  Linux

Command (m for help): c
DOS Compatibility flag is not set

Command (m for help): u
Changing display/entry units to sectors

Command (m for help): _
```

you could have up to four primary partitions, which would correspond to numbers 1 through 4. If you need more partitions you could redesignated one partition as an extended partition. after redesignated you could create logical partitions form extended partition. fdisk now supports the creation of more than 16 partitions on a drive. The remaining partitions are logical partitions, numbered 5 and above.

To create new partition type **n** press enter

If free space is available, fdisk normally starts the new partition at the first available sector or cylinder. The actual size of the partition depends on disk geometry. Press enter of First cylinder line

```
Command (m for help):
Command (m for help): n
First sector (18894848-25165823, default 18894848): _
```

give the size of partititon. Keep notice of format size. it is a + sign followed by size . K = Kilobyte M = Megabyte, G= Gigabyte . We want to create 100MB partition so give +100MB and press enter

```
[root@server ~]# fdisk /dev/sda
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help): n
First cylinder (1241-1567, default 1241):
Using default value 1241
Last cylinder, +cylinders or +size{K,M,G} (1241-1567, default 1567): +100M

Command (m for help): _
```

to save and exit type w and press enter

You may get temporary fail error if another partition on that drive has been formatted and mounted.

```
[root@server ~]# fdisk /dev/sda
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').

Command (m for help): n
First cylinder (1241-1567, default 1241):
Using default value 1241
Last cylinder, +cylinders or +size{K,M,G} (1241-1567, default 1567): +100M

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or res-
busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@server ~]# _
```

From command prompt you could try with partprobe command if linux is able to unmount existing partition it would return with success or if it is failed it would return with busy error message.

```
[root@server ~]# partprobe
Warning: WARNING: the kernel failed to re-read the partition table on /dev/sda (C
Device or resource busy). As a result, it may not reflect all of your changes u
ntil after reboot.
[root@server ~]# _
```

If you got failed message reboot system to take effect.

```
[root@server ~]# reboot -f _
```

After reboot login back with root and use **fdisk** command with **-l** switch

```
[root@server ~]# fdisk -l

Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf

      Device Boot   Start     End   Blocks Id System
/dev/sda1  *       1       26  204800  83 Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2       26     1046  8192000  83 Linux
/dev/sda3     1046     1177  1048576  82 Linux swap
/dev/sda4     1177     1567  3136512   5 Extended
/dev/sda5     1177     1241    512000  83 Linux
/dev/sda6     1241     1254    112275+  83 Linux
[root@server ~]# _
```

We have successfully created new partition /dev/sda6 but we would not be able to use it. Because it does not contain any filesystem. To make it useable we need to format it first. Ext4 was the default filesystem of RHEL6. From RHEL7 xfs is the default filesystem. The xfs filesystem reduces fragmentation, guarantees space for files, supports faster checks, and more. It even supports file timestamps in nanoseconds. It is proven technology. Given its speed and reliability, Red Hat even uses xfs as the default filesystem for partitions dedicated to the /boot directory. You can format it to the xfs filesystem using one of the following commands

```
# mkfs -t xfs /dev/sda6
# mke2fs -t xfs /dev/sda6
# mkfs.xfs /dev/sda6
```

Now create a mount point as given in question

```
[root@server ~]# mkdir /test
[root@server ~]# _
```

mount partition and test it. **lost+found** is a special directory and it automatically created on mount point of any partition.

```
[root@server ~]# mount /dev/sda6 /test
[root@server ~]# ls -a /test
. .. lost+found
[root@server ~]# _
```

Linux maintains filesystem information in **/etc/fstab** take its backup first

```
[root@server test]# cp /etc/fstab /etc/fstab.bk
[root@server test]# _
```

to mount this partition permanently open **/etc/fstab**

```
[root@server test]# vi /etc/fstab
```

make a entry for this partition in end of file

```
/dev/sda6 /test xfs defaults 0 0
```

to test reboot system and check mounted partition

```
[root@server ~]# cd /test
[root@server test]# ls
lost+found
[root@server test]#
```

Now we have created and mounted partition. You could use it.

how to delete partition from fdisk command

In our previous article we have created a simple partition of 100MB using fdisk command. Now in this article I would show you how you could delete partition using fdisk command.

Use **mount** command to locate mount point of partition.

```
[root@server ~]# mount
/dev/sda2 on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 on /boot type ext4 (rw)
/dev/sda5 on /home type ext4 (rw)
/dev/sda6 on /test type ext4 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
[root@server ~]#
```

As output show our newly created partition /dev/sda6 is mounted on /test. Before we remove any partition we need to unmount it. Use **umount** command to unmount it.



```
[root@server ~]# umount /test
[root@server ~]# mount
/dev/sda2 on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 on /boot type ext4 (rw)
/dev/sda5 on /home type ext4 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
[root@server ~]#
```

Now run **fdisk** command

```
[root@server ~]# fdisk /dev/sda
```

use **p** at fdisk command prompt to print current file system

```
[root@server ~]# fdisk /dev/sda
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
         switch off the mode (command 'c') and change display units to
         sectors (command 'u').

Command (m for help): p

Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf

      Device Boot   Start     End   Blocks   Id  System
/dev/sda1  *       1       26   204800   83  Linux
Partition 1 does not end on cylinder boundary.
/dev/sda2        26      1046   8192000   83  Linux
/dev/sda3      1046      1177   1048576   82  Linux swap / Solaris
/dev/sda4      1177      1567   3136512    5  Extended
/dev/sda5      1177      1241   512000   83  Linux
/dev/sda6      1241      1254    12275+   83  Linux

Command (m for help):
```

We want to delete /dev/sda6 partition use **d** at command prompt

```
[root@server ~]# fdisk /dev/sda
```

```
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
```

```
Command (m for help): p
```

```
Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	26	204800	83	Linux
Partition 1 does not end on cylinder boundary.						
/dev/sda2		26	1046	8192000	83	Linux
/dev/sda3		1046	1177	1048576	82	Linux swap / Solaris
/dev/sda4		1177	1567	3136512	5	Extended
/dev/sda5		1177	1241	512000	83	Linux
/dev/sda6		1241	1254	112275+	83	Linux

```
Command (m for help): d
```

Now give partition number which we want to delete in our case it would 6

```
switch off the mode (command 'c') and change display units to
sectors (command 'u').
```

```
Command (m for help): p
```

```
Disk /dev/sda: 12.9 GB, 12884901888 bytes
255 heads, 63 sectors/track, 1566 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000bf3bf
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	26	204800	83	Linux
Partition 1 does not end on cylinder boundary.						
/dev/sda2		26	1046	8192000	83	Linux
/dev/sda3		1046	1177	1048576	82	Linux swap / Solaris
/dev/sda4		1177	1567	3136512	5	Extended
/dev/sda5		1177	1241	512000	83	Linux
/dev/sda6		1241	1254	112275+	83	Linux

```
Command (m for help): d
```

```
Partition number (1-6): 6
```

Use w at command prompt

```
Disk identifier: 0x0000bf3bf

  Device Boot      Start        End      Blocks   Id  System
  /dev/sda1 *          1         26     204800   83  Linux
Partition 1 does not end on cylinder boundary.
  /dev/sda2          26        1046    8192000   83  Linux
  /dev/sda3       1046       1177    1048576   82  Linux swap / Solaris
  /dev/sda4       1177       1567    3136512    5  Extended
  /dev/sda5       1177       1241     512000   83  Linux
  /dev/sda6       1241       1254     12275+   83  Linux

Command (m for help): d
Partition number (1-6): 6

Command (m for help): w
The partition table has been altered!

Calling ioctl(0) to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
[root@server ~]#
```

As we have discussed in our previous article if kernel is unable to unmount the partition; it would return with error code 16. It require a reboot to locate new partition table. We should remove entry from fstab before do reboot. open /etc/fstab

remove entry from fstab

```
# /etc/fstab
# Created by anaconda on Sat Aug 11 19:06:28 2012
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=078a11a3-3078-43d5-b4a4-0ff99f184bc4 /           ext4      default
ts            1 1
UUID=56f99ced-0da2-4244-9976-42f61212ceca /boot        ext4      default
ts            1 2
UUID=55a76f14-28b4-43eb-8d8a-4b216a246646 /home        ext4      default
ts            1 2
UUID=1a2769c8-a5ac-480d-8f21-1b8b99670392 swap        swap      default
ts            0 0
tmpfs          /dev/shm           tmpfs      defaults      0 0
devpts         /dev/pts           devpts      gid=5,mode=620 0 0
sysfs          /sys               sysfs      defaults      0 0
proc           /proc              proc      defaults      0 0
/dev/sda6       /test              ext4      defaults      0 0

"/etc/fstab" 17L, 937C
```

after removing entry from fstab save file and quite.

```
# /etc/fstab
# Created by anaconda on Sat Aug 11 19:06:28 2012
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=878a11a3-3070-43d5-b4a4-0ff99f184bc4 / ext4 defaults
ts 1 1
UUID=56f99ced-0da2-4244-9976-42f61212ceca /boot ext4 defaults
ts 1 2
UUID=55a76f14-28b4-43eb-8d0a-4b216a246646 /home ext4 defaults
ts 1 2
UUID=1a2769c8-a5ac-480d-8f21-1b8b99670392 swap swap defaults
ts 0 0
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
:
:
:wq_
```

now reboot the system

```
[root@server ~]# reboot -f_
```

after restart check the status of mount point. As you have learnt from our previous article that if a partition is mounted on any directory, it would contain lost + found folder.

```
[root@server ~]# cd /test
[root@server test]# ls -a
[root@server test]# _
```

What is LVM

Logical volume management provides a higher-level view of the disk storage on a computer system than the traditional view of disks and partitions. This gives the system administrator much more flexibility in allocating storage to applications and users.

The logical volume manager also allows management of storage volumes in user-defined groups, allowing the system administrator to deal with sensibly named volume groups such as "development" and "sales" rather than physical disk names such as "sda" and "sdb".

Advantage of Logical Volume Management

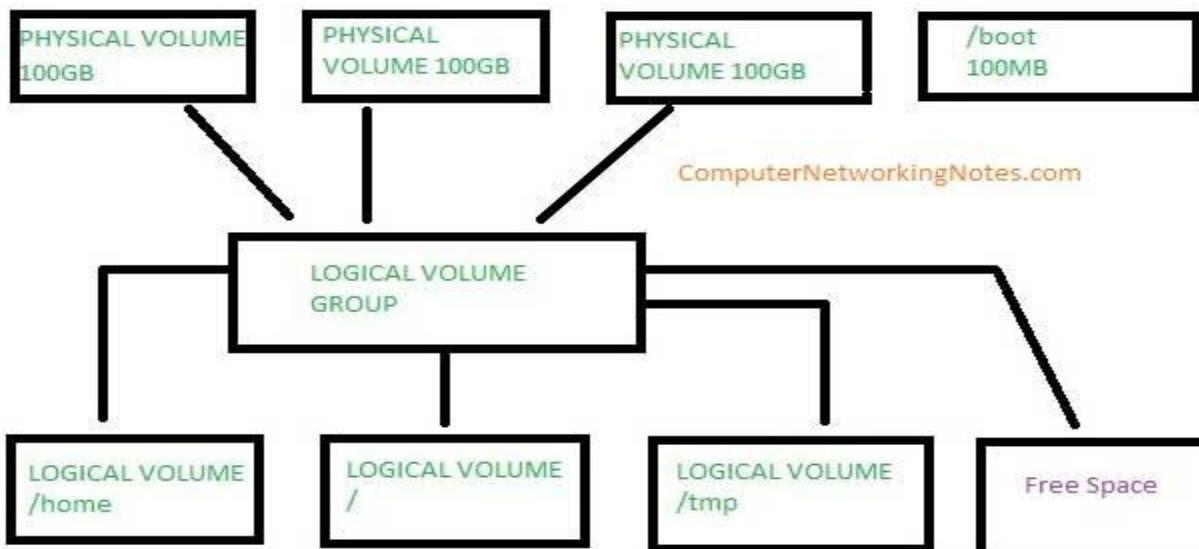
One of the difficult decisions facing a new user installing Linux for the first time is how to partition the disk drive. The need to estimate just how much space is likely to be needed for system files and user files makes the installation more complex than is necessary and some users simply opt to put all their data into one large partition in an attempt to avoid the issue.

Once the user has guessed how much space is needed for /home /usr / (or has let the installation program do it) then is quite common for one of these partitions to fill up even if there is plenty of disk space in one of the other partitions.

With logical volume management, the whole disk would be allocated to a single volume group and logical volumes created to hold the / /usr and /home file systems. If, for example the /home logical volume later filled up but there was still space available on /usr then it would be possible to shrink /usr by a few megabytes and reallocate that space to /home.

Another alternative would be to allocate minimal amounts of space for each logical volume and leave some of the disk unallocated. Then, when the partitions start to fill up, they can be expanded as necessary.

LVM allows administrators to divide hard drive space into physical volumes (PV), which can then be combined into logical volume groups (VG), which are then divided into logical volumes (LV) on which the filesystem and mount point are created.





As shown in image because a logical volume group can include more than one physical volume, a mount point can include more than one physical hard drive, meaning the largest mount point can be larger than the biggest hard drive in the set. These logical volumes can be resized later if more disk space is needed for a particular mount point. After the mount points are created on logical volumes, a filesystem must be created on them.

LVM is used by default during installation for all mount points except the /boot partition, which cannot exist on a logical volume. But you could create LVM after the installation. In our next article I would show you how to create and update LVM in rhce exam.

Creating LVM in RedHat Linux

LVM(Logical Volume Manager): LVM provides a flexible and high level approach to managing disk space. Instead of each disk drive being split into partitions of fixed sizes onto which fixed size file systems are created, LVM provides a way to group together disk space into logical volumes which can be easily re-sized and moved. In addition LVM allows administrators to carefully control disk space assigned to different groups of users by allocating distinct volume groups or logical volumes to those users. When the space initially allocated to the volume is exhausted the administrator can simply add more space without having to move the user files to a different file system. LVM have partition id 8e.

Following steps are followed to create LVM.

1. Create PV
2. Create VG
3. Create LVM
4. Format LVM & mount it.

1. Create PV(Physical Volume):

```
#fdisk -cul
```

```
Disk /dev/sda: 120.0 GB, 120034123776 bytes
255 heads, 63 sectors/track, 14593 cylinders, total 234441648 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000a808c
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	2048	206847	102400	83	Linux
/dev/sda2		206848	57550847	28672000	83	Linux
/dev/sda3		58605120	64227869	2811375	83	Linux
/dev/sda4		57552896	57960446	203775+	83	Linux

In above output there is three Linux partitions, from these given partition we are going to create new physical volume by using sda3 & sda4.



```
#pvcreate /dev/sda3
```

```
#pvcreate /dev/sda4
```

To show the new physical volume we use following syntax

```
#pvdisplay
```

output :

```
--- Physical volume ---
```

PV Name	/dev/sda3
VG Name	
PV Size	2.34 GiB / not usable 32.00 MiB
Allocatable	yes
PE Size	4.00 MiB
Total PE	874
Free PE	97
Allocated PE	777
PV UUID	xL33Gt-pBB3-4XdC-7BnK-QSZh-6Xyl-T0fSh

```
--- Physical volume ---
```

PV Name	/dev/sda4
VG Name	
PV Size	2.68 GiB / not usable 1.48 MiB
Allocatable	yes
PE Size	4.00 MiB
Total PE	686
Free PE	436
Allocated PE	250
PV UUID	0gJH6J-sg0N-XeSh-rwcd-6DK0-CXef-0gt6vw

2. Create VG(Volume Group)

```
#vgcreate vol0 /dev/sda3 /dev/sda4
```

in above syntax here vol0 is VG label. To display new volume group

```
#vgdisplay
```



Output :

```
-- Volume group --
VG Name          vol0
System ID
Format           lvm2
Metadata Areas   1
Metadata Sequence No 4
VG Access        read/write
VG Status         resizable
MAX LV            0
Cur LV            3
Open LV           2
Max PV            0
Cur PV            1
Act PV            1
VG Size           27.31 GiB
PE Size           32.00 MiB
Total PE          874
Alloc PE / Size   777 / 24.28 GiB
Free PE / Size    97 / 3.03 GiB
VG UUID          v4zfUr-nEh4-JKyu-xcge-RRlp-O0kp-HQVCT3
```



3. Create LVM

```
#lvcreate -size 240M -name lv1 vol0
```

by using above syntax this will create 240Mb size new lvm and here lv1 is label of new lvm. To display information of this volume use following syntax

```
#lvdiskdisplay
```

Output :

```
-- Logical volume --
LV Name          /dev/vol0/lv1
VG Name          vol0
LV UUID          2sXIPe-AIDg-WFMy-ijzb-UUBS-Tj6H-IKGLDb
LV Write Access  read/write
LV Status         available
# open            1
LV Size           240.00 MiB
Current LE        16
Segments          1
Allocation        inherit
```

Read ahead sectors	auto
- currently set to	256
Block device	253:2

4. now need to format lvm and mount it.

```
#mkfs.ext4 /dev/vol0/lv1
```

Above syntax will format lv1 in ext4 filesystem. Now need to mount this drive.

```
#mount /dev/vol0/lv1 /media/lv
```

Note:- We can **extend** and **reduce** lvm size according to our requirement.

1. Extend LVM :

* **extend lvm**

```
#lvextend --size +40M /dev/vol0/home
```

Output :

Rounding up size to full physical extent 40.00 MiB

Extending logical volume lv1 to 280.00 MiB

Logical volume home successfully resized

*** resize file system**

```
#resize2fs /dev/vol0/lv1
```

Output :

resize2fs 1.41.12 (17-May-2010)

Filesystem at /dev/vol0/lv1 is mounted on /media/lv; on-line resizing required

old_desc_blocks = 1, new_desc_blocks = 1

Performing an on-line resize of /dev/vol0/lv1 to 147456 (4k) blocks.

The filesystem on /dev/vol0/lv1 is now 147456 blocks long.

2. Reduce lvm size : To reduce any partition need to follow these steps.

* unmount partition

* scan file system

* resize file system by 60Mb

* lvreduce

* mount reduced partition

*** unmount partition :**

```
[root@desktop13 ~]# umount /dev/vol0/lv1
```

*** scan file system :**



```
[root@desktop13 ~]# e2fsck -f /dev/vol0/lv1
e2fsck 1.41.12 (17-May-2010)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/vol0/lv1: 27/40960 files (0.0% non-contiguous), 6787/147456 blocks
```

* **resize file system by 60Mb**

```
[root@desktop13 ~]# resize2fs /dev/vol0/lv1 60M
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/vol0/lv1 to 15360 (4k) blocks.
The filesystem on /dev/vol0/lv1 is now 15360 b
```

* **lvreduce :**

```
[root@desktop13 ~]# lvreduce --size 60M /dev/vol0/lv1
```

```
Rounding up size to full physical extent 64.00 MiB
WARNING: Reducing active and open logical volume to 64.00 MiB
THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce lv1? [y/n]: y
Reducing logical volume lv1 to 64.00 MiB
Logical volume lv1 successfully resized
```

* **mount reduced partition**

```
[root@desktop13 ~]# mount /dev/vol0/lv1 /media/lv
now we have new lvm size of 60Mb.
```

LVM(Logical Volume Manager): LVM provides a flexible and high level approach to managing disk space. Instead of each disk drive being split into partitions of fixed sizes onto which fixed size file systems are created, LVM provides a way to group together disk space into logical volumes which can be easily re-sized and moved. In addition LVM allows administrators to carefully control disk space assigned to different groups of users by allocating distinct volume groups or logical volumes to those users. When the space initially allocated to the volume is exhausted the administrator can simply add more space without having to move the user files to a different file system. LVM have partition id 8e.

Following steps are followed to create LVM.

1. Create PV
2. Create VG
3. Create LVM
4. Format LVM & mount it.

1. Create PV(Physical Volume):

```
#fdisk -cul
```

Disk /dev/sda: 120.0 GB, 120034123776 bytes
 255 heads, 63 sectors/track, 14593 cylinders, total 234441648 sectors
 Units = sectors of 1 * 512 = 512 bytes
 Sector size (logical/physical): 512 bytes / 512 bytes
 I/O size (minimum/optimal): 512 bytes / 512 bytes
 Disk identifier: 0x000a808c

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	2048	206847	102400	83	Linux
/dev/sda2		206848	57550847	28672000	83	Linux
/dev/sda3		58605120	64227869	2811375	83	Linux
/dev/sda4		57552896	57960446	203775+	83	Linux

In above output there is three Linux partitions, from these given partition we are going to create new physical volume by using sda3 & sda4.

```
#pvcreate /dev/sda3
```

```
#pvcreate /dev/sda4
```

To show the new physical volume we use following syntax

```
#pvdisplay
```

output :

--- Physical volume ---

PV Name	/dev/sda3
VG Name	
PV Size	2.34 GiB / not usable 32.00 MiB
Allocatable	yes
PE Size	4.00 MiB
Total PE	874
Free PE	97
Allocated PE	777
PV UUID	xL33Gt-pBB3-4XdC-7BnK-QSZk-6Xyl-T0fSh

--- Physical volume ---

PV Name	/dev/sda4
VG Name	
PV Size	2.68 GiB / not usable 1.48 MiB
Allocatable	yes
PE Size	4.00 MiB
Total PE	686



Free PE 436
Allocated PE 250
PV UUID 0gJH6J-sg0N-XeSh-rwcd-6DK0-CXef-0gt6vw



2. Create VG(Volume Group)

```
#vgcreate vol0 /dev/sda3 /dev/sda4
```

in above syntax here vol0 is VG label. To display new volume group

```
#vgdisplay
```

Output :

```
--- Volume group ---
VG Name          vol0
System ID
Format           lvm2
Metadata Areas   1
Metadata Sequence No  4
VG Access        read/write
VG Status         resizable
MAX LV            0
Cur LV             3
Open LV            2
Max PV             0
Cur PV             1
Act PV             1
VG Size           27.31 GiB
PE Size            32.00 MiB
Total PE          874
Alloc PE / Size   777 / 24.28 GiB
Free PE / Size    97 / 3.03 GiB
VG UUID           v4zfUr-nEh4-JKyu-xcge-RRlp-O0kp-HQVCT3
```

3. Create LVM

```
#lvcreate --size 240M --name lv1 vol0
```

by using above syntax this will create 240Mb size new lvm and here lv1 is label of new lvm. To display information of this volume use following syntax

```
#lvdiskdisplay
```

Output :

--- Logical volume ---



LV Name	/dev/vol0/lv1
VG Name	vol0
LV UUID	2sXIPe-AIDg-WFMy-ijzb-UUBS-Tj6H-IKGLDb
LV Write Access	read/write
LV Status	available
# open	1
LV Size	240.00 MiB
Current LE	16
Segments	1
Allocation	inherit
Read ahead sectors	auto
- currently set to	256
Block device	253:2

4. now need to format lvm and mount it.

```
#mkfs.ext4 /dev/vol0/lv1
```

Above syntax will format lv1 in ext4 filesystem. Now need to mount this drive.

```
#mount /dev/vol0/lv1 /media/lv
```

Note:- We can extend and reduce lvm size according to our requirement.

1. Extend LVM :

```
* extend lvm
```

```
#lvextend --size +40M /dev/vol0/home
```

Output :

```
Rounding up size to full physical extent 40.00 MiB
```

```
Extending logical volume lv1 to 280.00 MiB
```

```
Logical volume home successfully resized
```

* resize file system

```
#resize2fs /dev/vol0/lv1 - This is for RHEL6
```

```
#xfs-growfs /dev/vol0/lv1 - This is for RHEL7
```

Output :

```
resize2fs 1.41.12 (17-May-2010)
```

```
Filesystem at /dev/vol0/lv1 is mounted on /media/lv; on-line resizing required
```

```
old_desc_blocks = 1, new_desc_blocks = 1
```

```
Performing an on-line resize of /dev/vol0/lv1 to 147456 (4k) blocks.
```

```
The filesystem on /dev/vol0/lv1 is now 147456 blocks long.
```

2. Reduce lvm size : To reduce any partition need to follow these steps.

- * umount partition
- * scan file system
- * resize file system by 60Mb
- * lvreduce
- * mount reduced partition

* umount partition :

```
[root@desktop13 ~]# umount /dev/vol0/lv1
```

* scan file system :

```
[root@desktop13 ~]# e2fsck -f /dev/vol0/lv1  
e2fsck 1.41.12 (17-May-2010)
```

Pass 1: Checking inodes, blocks, and sizes

Pass 2: Checking directory structure

Pass 3: Checking directory connectivity

Pass 4: Checking reference counts

Pass 5: Checking group summary information

```
/dev/vol0/lv1: 27/40960 files (0.0% non-contiguous), 6787/147456 blocks
```

* resize file system by 60Mb

```
[root@desktop13 ~]# resize2fs /dev/vol0/lv1 60M  
resize2fs 1.41.12 (17-May-2010)
```

Resizing the filesystem on /dev/vol0/lv1 to 15360 (4k) blocks.

The filesystem on /dev/vol0/lv1 is now 15360 b

* lvreduce :

```
[root@desktop13 ~]# lvreduce --size 60M /dev/vol0/lv1
```

Rounding up size to full physical extent 64.00 MiB

WARNING: Reducing active and open logical volume to 64.00 MiB

THIS MAY DESTROY YOUR DATA (filesystem etc.)

Do you really want to reduce lv1? [y/n]: y

Reducing logical volume lv1 to 64.00 MiB

Logical volume lv1 successfully resized

* mount reduced partition

```
[root@desktop13 ~]# mount /dev/vol0/lv1 /media/lv  
now we have new lvm size of 60Mb
```

Network administration

Redhat test your ability to configure several networking related services during the RHCE Exam. To pass RHCE Exam you must have to understand networking.

Linux is designed for networking. Networking is the vast topic. We have simplified this section for RHCE Exam. We would start from IP address. Every computer in network requires an IP address to communicate with other computer

IP address

Every computer on network requires an IP address to communicate with other computer. Linux is developed for networking. To pass RHCE exam you must understand networking.

An IP is a 32-bit number comprised of a host number and a network prefix, both of which are used to uniquely identify each node within a network.

To make these addresses more readable, they are broken up into 4 bytes, or octets, where any 2 bytes are separated by a period. This is commonly referred to as dotted decimal notation.

The first part of an Internet address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This creates the two-level addressing hierarchy.

All hosts on a given network share the same network prefix but must have a unique host number. Similarly, any two hosts on different networks must have different network prefixes but may have the same host number.

Here is a simple example of an IP address: 192.168.1.1

An additional value, called a subnet mask, determines the boundary between the network and host components of an address.

Subnet masks are 32 bits long and are typically represented in dotted-decimal (such as 255.255.255.0) or the number of networking bits (such as /24). The networking bits in a mask must be contiguous and the host bits in the subnet mask must be contiguous. 255.0.255.0 is an invalid mask. A subnet mask is used to mask a portion of the IP address, so that TCP/IP can tell the difference between the network ID and the host ID. TCP/IP uses the subnet mask to determine whether the destination is on a local or remote network.

- Class A subnet mask 255.0.0.0
- Class B subnet mask 255.255.0.0
- Class C subnet mask 255.255.255.0

When dealing with IP addresses, the address is broken into two components:

- Network component Defines on what segment, in the network, a device is located
- Host component Defines the specific device on a particular network segment

The network number uniquely identifies a segment in the network and a host number uniquely identifies a device on a segment. The combination of these two numbers must be unique throughout the entire network.

IP addresses are divided in five class.

Class A addresses range from 1-126
Class B addresses range from 128-191
Class C addresses range from 192-223
Class D addresses range from 224-239
Class E addresses range from 240-254

0 is reserved and represents all IP addresses;
127 is a reserved address and is used for loop back testing;
255 is a reserved address and is used for broadcasting purposes.

decimal notation

For example

- IP address 159.123.12.2 belongs to class B because 159 [First number] falls in range 128 - 191
- IP address 15.12.12.6 belongs to class A because 15 [First number] falls in range 1 - 126
- IP address 192.168.1.2 belongs to class C because 192 [First number] falls in range 192 - 223

When you are dealing with IP addresses, two numbers are always reserved for each network number:

The first address in the network represents the network's address, and the last address in the network represents the broadcast address for this network, called directed broadcast.

When you look at IP itself, two IP addresses are reserved: 0.0.0.0 (the very first address), which represents all IP addresses, and 255.255.255.255 (the very last address), which is the local broadcast address.

As to assigning addresses to devices, two general types of addresses can be used: public and private.

Public addresses

Public addresses are Class A, B, and C addresses that can be used to access devices in other public networks, such as the Internet.

Private Addresses

Within the range of addresses for Class A, B, and C addresses are some reserved addresses, commonly called private addresses. Anyone can use private addresses; however, this creates a problem if you want to access the Internet. Remember that each device in the network (in this case, this includes the Internet) must have a unique IP address. If two networks are using the same private addresses, you would run into reachability issues. To access the Internet, your source IP addresses must have a unique Internet public address. This can be accomplished through address translation. Here is a list of private addresses.

Class A: 10.0.0.0-10.255.255.255 (1 Class A network)
Class B: 172.16.0.0-172.31.255.255 (16 Class B networks)
Class C: 192.168.0.0-192.168.255.255 (256 Class C networks)

(Internet Protocol) addressing methods.

Static /Dynamic

Each device in an IP network is either assigned a permanent address (static) by the network administrator or is assigned a temporary address (dynamic) via DHCP software. Routers, firewalls and proxy servers use static addresses as do most



servers and printers that serve multiple users. Client machines may use static or dynamic IP addresses. The IP address assigned to your service by your cable or DSL Internet provider is typically dynamic IP. In routers and operating systems, the default configuration for clients is dynamic IP.

DHCP

DHCP stands for Dynamic Host Configuration Protocol. This protocol assigns network IP addresses to clients on the network at startup. With DHCP, each client workstation does not need to be set up with a static IP address. DHCP is recommended on large networks. It would be very time consuming to manually assign a static IP address to every workstation on your network. With static IP addressing, the IP address that you assign to a device never changes. A DHCP server contains a pool of IP addresses that it can draw from to assign to devices that are connecting to the network. Other TCP/IP properties, such as default gateways, DNS servers, and subnet masks can also be assigned automatically.

IPv6

Network industry is moving to adopt new version of IPv6. IPv6 have several new features. RHCE exam test you networking skills on IPv4 so we are not including IPv6 in this article. We have a separate section for IPv6.

How to assign IP address in Linux

Every computer requires IP configuration in network.

Four configuration parameters are required.

- IP Address
- Netmask
- Default Gateway or Router
- DNS Server(s)

In RHEL you can assign these parameters in two ways.

- Static configuration
- Dynamic configuration
- Dynamic configuration

Static configuration

In static configuration you have to assign all these parameters manually. Static configuration does not change automatically. Static configuration generally used with servers or network resources like printer, router etc. Static configuration uses set parameters for the configuration, which is known by the system and the network.

Dynamic configuration

Dynamic configurations are handled by DHCP server. In dynamic configuration DHCP service on the network provides all these parameters to a system when it joins the network.

Dynamic configuration generally used with workstations. Dynamic configuration configures network parameters on the boot.

Red Hat provides two tools to configure the network device.

- Network configuration tool
- Network manager

Network configuration tool

This is a command line network configuration tool. Use this tool to configure IP address on console. This tool can be invoked by running system-config-network command.

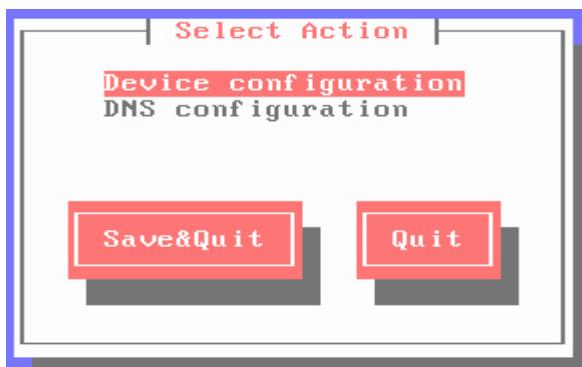
```
#system-config-network
#system-config-network

Red Hat Enterprise Linux Server release 6.1 (Santiago)
Kernel 2.6.32-131.0.15.el6.x86_64 on an x86_64

Server login: root
Password:
[root@Server ~]# system-config-network_
```

Key control

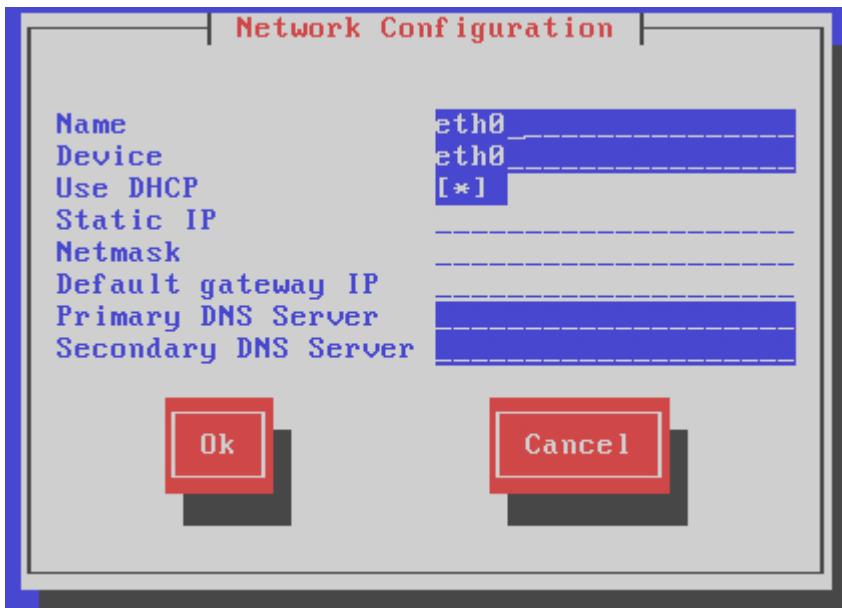
- TAB Key :- To switch between options
- Enter /Space :- Select the highlighted options
- Select Device Configuration if other option is selected press TAB key until device configuration is selected and press ENTER



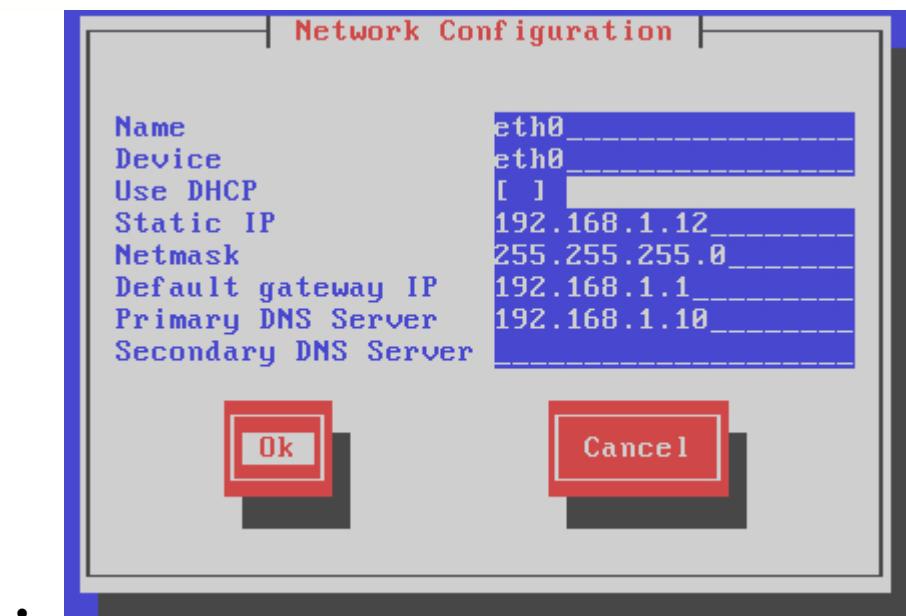
- On Select A Device screen select first network card (eth0) and press ENTER



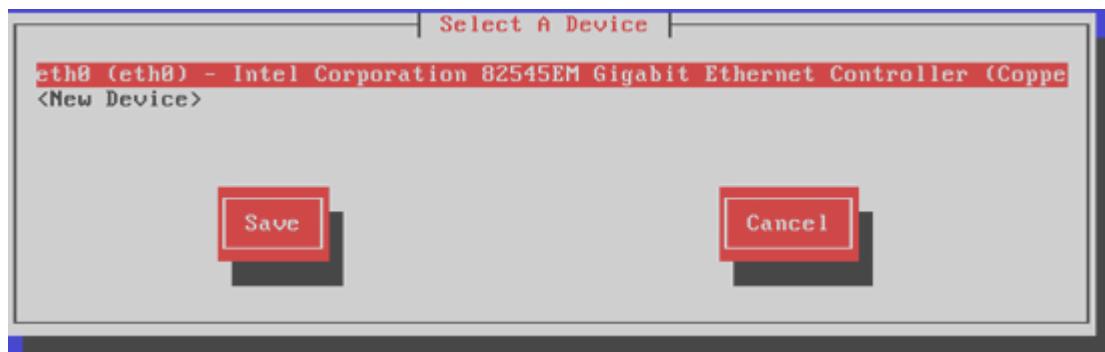
- Now we are on Network configuration screen. As we mentioned above IP configuration can be set in two ways static or dynamic.
- To set IP configuration dynamically Select DHCP



- To use static IP configuration press TAB key to highlight DHCP option and press SPACEBAR to deselect it. Fill necessary parameters and select Ok by pressing TAB key. Once OK is highlighted press ENTER



- Select Save by pressing TAB key and press ENTER



- Select Save & Quit by pressing TAB key and press ENTER



- To put the configuration customized with this tool into effect we need to reactivate the associated device. Until we reactivate associated device it would run with old configuration. You can check it with ifconfig command

```
[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.22.134 Bcast:192.168.22.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:6031 errors:0 dropped:0 overruns:0 frame:0
             TX packets:3289 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:6370560 (6.0 MiB) TX bytes:352056 (343.8 KiB)

[root@Server ~]# _
```

- Use ifdown command to deactivate and ifup to activate.

```
[root@Server ~]# ifdown eth0
Device state: 3 (disconnected)
[root@Server ~]# ifup eth0
Active connection state: activating
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/7
state: activated
Connection activated
[root@Server ~]# _
```

- Check again with ifconfig command. The configuration of the network card should reflect the new configuration.

```
[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.1.12 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:6032 errors:0 dropped:0 overruns:0 frame:0
             TX packets:3432 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:6370620 (6.0 MiB) TX bytes:364438 (355.8 KiB)
```

- [root@Server ~]# _

• Network manager tool

This is a GUI tool to configure IP address. It is also default network management tool for RHEL6. Use this tool to configure IP address on GUI. To invoke this tool click System | Preferences | Network Connections.



Applications Places

System Preferences >
Administration >
Documentation >
Help
About this Computer
Log Out root...
Shut Down...

- About Me
- Appearance
- Assistive Technologies
- Bluetooth
- Default Printer
- Desktop Effects
- Display
- File Management
- Input Method
- Keyboard
- Keyboard Shortcuts
- Mouse
- Network Connections
- Network Device



You can also invoke this tool from terminal. Run following command

```
#nm-connection-editor
```

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# nm-connection-editor
```

This command may return with following error

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# nm-connection-editor  
** (nm-connection-editor:6737): WARNING **: get_all_cb: couldn't retrieve system  
settings properties: (2) The name org.freedesktop.NetworkManagerSystemSettings  
was not provided by any .service files.  
** (nm-connection-editor:6737): WARNING **: fetch_connections_done: error fetchi  
ng system connections: (2) The name org.freedesktop.NetworkManagerSystemSettings  
was not provided by any .service files.
```

This error triggered when NetworkManager service is disabled.

System 

root@Server:~

```
File Edit View Search Terminal Help
[root@Server ~]# chkconfig --list NetworkManager
NetworkManager 0:off 1:off 2:on 3:on 4:on 5:on 6:off
[root@Server ~]# service NetworkManager status
NetworkManager is stopped
[root@Server ~]# If service is stopped no network icon would be present
```

Start NetworkManager service

System 

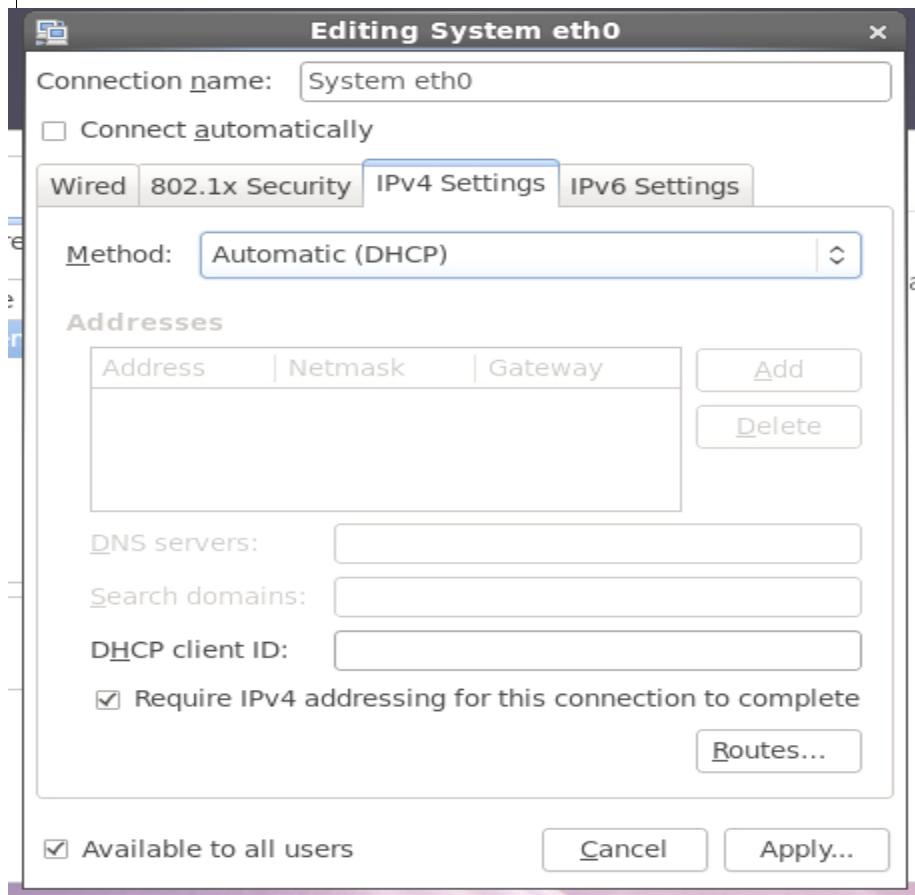
root@Server:~

```
File Edit View Search Terminal Help
[root@Server ~]# chkconfig --list NetworkManager
NetworkManager 0:off 1:off 2:on 3:on 4:on 5:on 6:off
[root@Server ~]# service NetworkManager status
NetworkManager is stopped
[root@Server ~]# service NetworkManager start
Setting network parameters... [ OK ]
Starting NetworkManager daemon: [ OK ]
[root@Server ~]# Network icon would appear once service is started
```

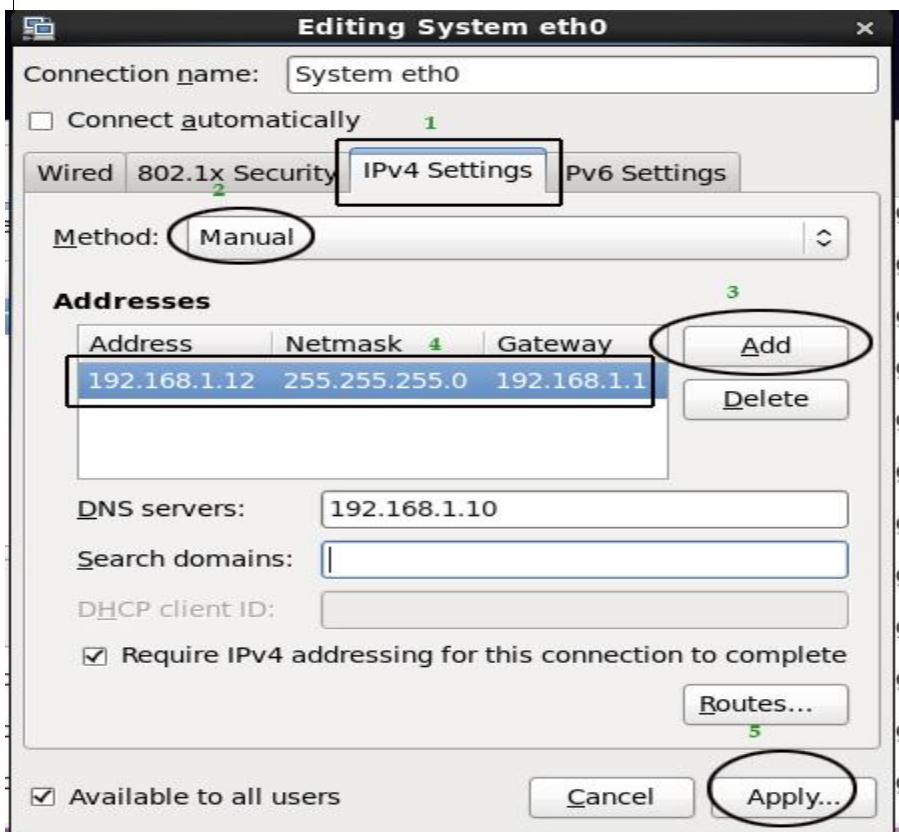
Now try to invoke network manager again. From open window select eth0 and click on edit



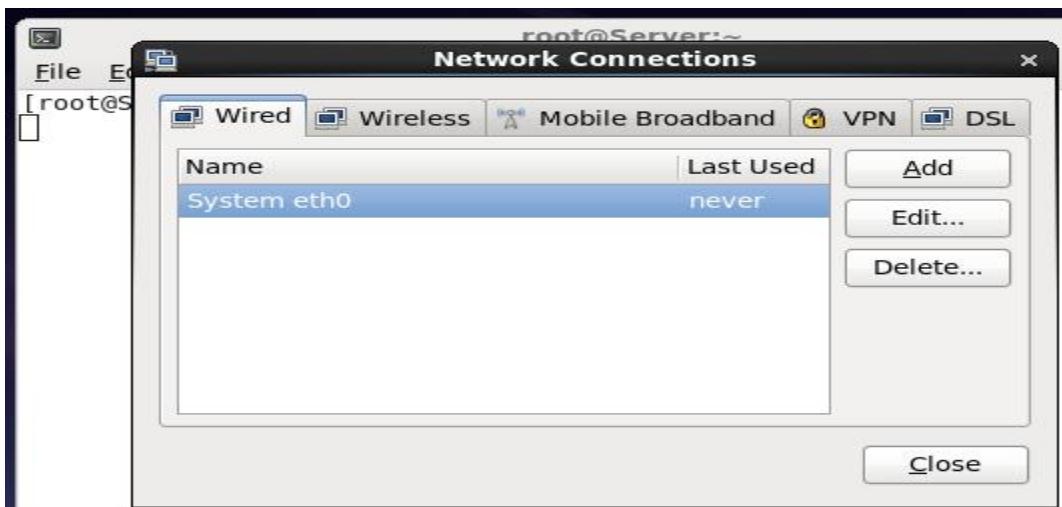
Click on IPv4 tab. For dynamic configuration select DHCP from method drop down



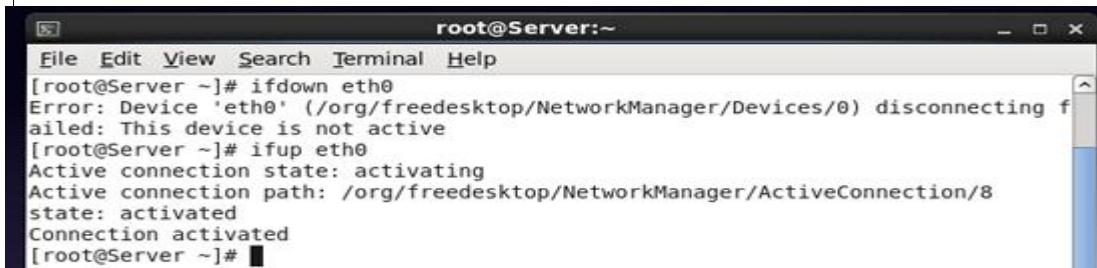
For static configuration select Manual from drop down and click on Add button, fill IP configuration and click on apply button



We are back on Network Connection window click on close

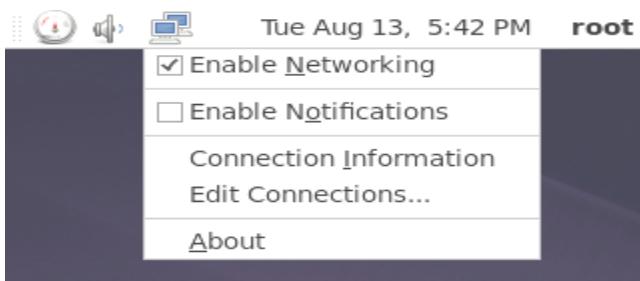


Reactivate network adaptor so new configuration can take effect.

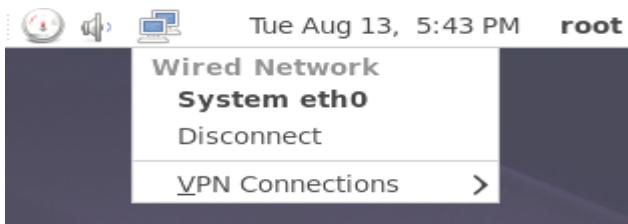


```
root@Server:~#
File Edit View Search Terminal Help
[root@Server ~]# ifdown eth0
Error: Device 'eth0' (/org/freedesktop/NetworkManager/Devices/0) disconnecting failed: This device is not active
[root@Server ~]# ifup eth0
Active connection state: activating
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/8
state: activated
Connection activated
[root@Server ~]#
```

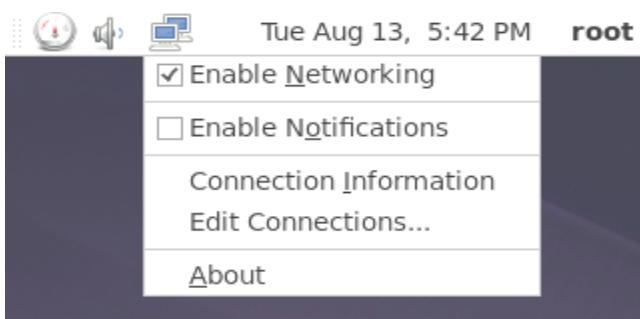
You can also invoke Network Manager directly from panel .Right click on Network icon and click on edit connection



To deactivate do left click on network icon and click on Disconnect



To activate do left click on network icon and click on network adaptor



Both tools are available during the exam. Do practice with both.

Networking tools

In Linux several networking tools are available to manage the network. RHCE exam include several networking related questions. During the exam you need to configure the network. For RHCE exam you must know the following commands and their uses.

- ifconfig

- [ifup](#)
- [ifdown](#)
- [ping](#)
- [arp](#)
- [netsat -r](#)
- [route -n](#)
- [dhclient](#)
- [system-config-network](#)
- [service network \[start\]\[restart\]](#)
- [chkconfig --list network](#)
- [chkconfig network on](#)

ifconfig

Every computer in network requires an IP address. With **ifconfig** command you can easily check the current configuration of active network adapters.

#ifconfig

```
root@Server:~#
File Edit View Search Terminal Help
[root@Server ~]# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.22.134 Bcast:192.168.22.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:3612 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2288 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2101239 (2.0 MiB) TX bytes:231630 (226.2 KiB)

lo      Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 b) TX bytes:960 (960.0 b)

[root@Server ~]#
```

Default **ifconfig** command would display the current state of all active network adapters. To display the current configuration of a specific adapter use its number with **ifconfig** command. For example to display the current configuration of first adaptor only run following command

#ifconfig eth0

```
root@Server:~ 
File Edit View Search Terminal Help
[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.22.134 Bcast:192.168.22.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:3612 errors:0 dropped:0 overruns:0 frame:0
             TX packets:2288 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:2101239 (2.0 MiB) TX bytes:231630 (226.2 KiB)

[root@Server ~]#
```

During the exam if you think **ifconfig** command is missing any network adaptor, use **-a** option to list the configuration of all network adaptors, whether or not they are currently active.

```
#ifconfig -a
```

Other use of ifconfig command

How to assign IP address from ifconfig command

ifconfig command can also be used to assign the IP address. For example to assign IP address and subnet mask to **eth0** adapter run following command

```
#ifconfig eth0 192.168.1.34 netmask 255.255.255.0
```

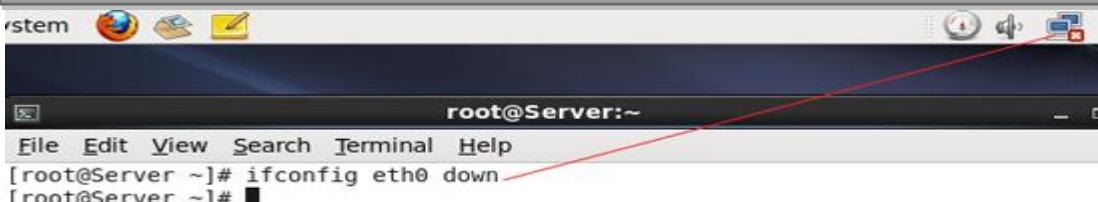
```
root@Server:~ 
File Edit View Search Terminal Help
[root@Server ~]# ifconfig eth0 192.168.1.34 netmask 255.255.255.0
[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.1.34 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:5453 errors:0 dropped:0 overruns:0 frame:0
             TX packets:3313 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:2868605 (2.7 MiB) TX bytes:346094 (337.9 KiB)

[root@Server ~]#
```

How to activate or deactivate network adapter from ifconfig command

With **ifconfig** command you can also activate or deactivate the network adaptor. To deactivate network adaptor run following command

```
#ifconfig [network adaptor] down
```



```
root@Server:~ 
File Edit View Search Terminal Help
[root@Server ~]# ifconfig eth0 down
[root@Server ~]#
```

To activate the network adaptor run following command

```
#ifconfig [network adaptor] up
```



```
File Edit View Search Terminal Help
[root@Server ~]# ifconfig eth0 down
[root@Server ~]# ifconfig eth0 up
[root@Server ~]#
```

During the exam use **ifconfig** command to list the current configuration of network adaptors only. There are better tools available for above tasks. To assign IP address use **system-config-network**. To activate or deactivate network adapter use **ifup** and **ifdown** commands.

ifdown

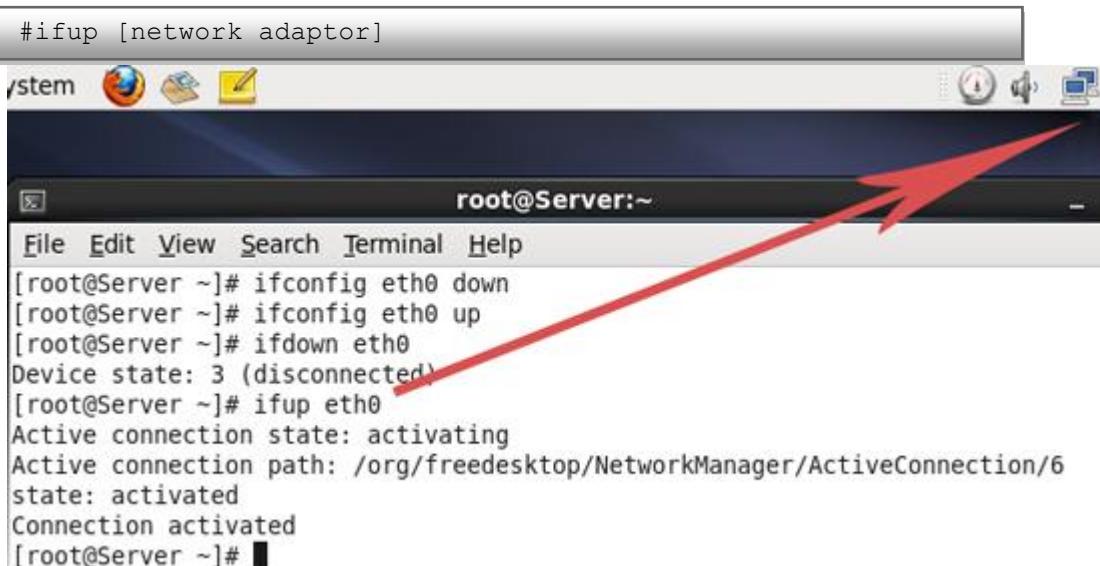
ifdown command is used to deactivate the network adaptor. syntax of **ifdown** is following



```
#ifdown [network adaptor]
File Edit View Search Terminal Help
[root@Server ~]# ifconfig eth0 down
[root@Server ~]# ifconfig eth0 up
[root@Server ~]# ifdown eth0
Device state: 3 (disconnected)
[root@Server ~]#
```

ifup

ifup command is used to activate the network adaptor. syntax of **ifup** is following



```
#ifup [network adaptor]
File Edit View Search Terminal Help
[root@Server ~]# ifconfig eth0 down
[root@Server ~]# ifconfig eth0 up
[root@Server ~]# ifdown eth0
Device state: 3 (disconnected)
[root@Server ~]# ifup eth0
Active connection state: activating
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/6
state: activated
Connection activated
[root@Server ~]#
```

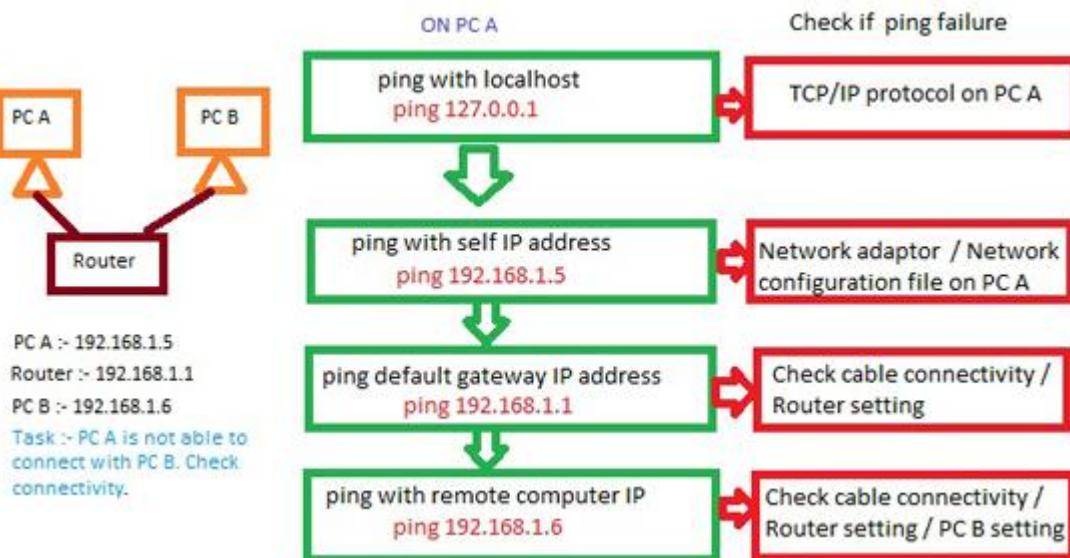
ping

ping command is used to test the connectivity. **ping** command on linux works continuously. We need to press CTRL+C to stop it. If you are connected with internet, you can also check the connectivity with website. For example to test connectivity with our site run following command

```
#ping www.computernetworkingnotes.com
root@Server:~#
File Edit View Search Terminal Help
[root@Server ~]# ping www.computernetworkingnotes.com
PING cf-protected-www.computernetworkingnotes.com.cdn.cloudflare.net (108.162.196.119) 56(84) bytes of data.
64 bytes from 108.162.196.119: icmp_seq=1 ttl=128 time=120 ms
64 bytes from 108.162.196.119: icmp_seq=2 ttl=128 time=151 ms
^C
--- cf-protected-www.computernetworkingnotes.com.cdn.cloudflare.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1183ms
rtt min/avg/max/mdev = 120.147/136.010/151.873/15.863 ms
[root@Server ~]# ping 108.162.196.119
PING 108.162.196.119 (108.162.196.119) 56(84) bytes of data.
64 bytes from 108.162.196.119: icmp_seq=1 ttl=128 time=158 ms
64 bytes from 108.162.196.119: icmp_seq=2 ttl=128 time=180 ms
64 bytes from 108.162.196.119: icmp_seq=3 ttl=128 time=155 ms
64 bytes from 108.162.196.119: icmp_seq=4 ttl=128 time=172 ms
64 bytes from 108.162.196.119: icmp_seq=5 ttl=128 time=184 ms
^C
--- 108.162.196.119 ping statistics ---
6 packets transmitted, 5 received, 16% packet loss, time 5201ms
rtt min/avg/max/mdev = 155.244/170.301/184.868/11.672 ms
[root@Server ~]#
```

During the exam you will not have internet access. **ping** command works on local network as well. Whenever you have trouble in connecting with network, use **ping** command in following order.

- ping with localhost
- ping with self IP address
- ping with default gateway IP address
- ping with remote computer IP



arp

Address resolution protocol (ARP) bind MAC address with IP address. ARP protocol works only in local network as MAC address are not routable. ARP table keep entries of local network systems. It is helpful to detect duplicate address on the network.



Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.22.2	ether	00:50:56:eb:f1:5b	C		eth0

- The Address column lists detected IP addresses on the network.
- The HWtype column shows the hardware type of the adapter.
- The HWaddress column shows the hardware address of the adapter.

netsat -r and route -n

netstat command with **-r** option is equivalent to the **route** command with **-n** option. Both will display the routing table.

```
root@Server:~ [File Edit View Search Terminal Help]
[root@Server ~]# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask        Flags MSS Window irtt Iface
192.168.22.0   *              255.255.255.0 U        0 0          0 eth0
default        192.168.22.2   0.0.0.0       UG       0 0          0 eth0
[root@Server ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
192.168.22.0   0.0.0.0       255.255.255.0 U      1    0      0 eth0
0.0.0.0         192.168.22.2  0.0.0.0       UG      0    0      0 eth0
[root@Server ~]#
```

Routing table can be very helpful during the exam to detect misconfigured gateway.

dhclient

dhclient command fetch IP configuration for calling network card. For example following command will fetch IP configuration for eth0 network card from DHCP server.

```
root@Server:~ [File Edit View Search Terminal Help]
[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.1.23 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b) TX bytes:4134 (4.0 KiB)

[root@Server ~]# dhclient eth0
[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.22.134 Bcast:192.168.22.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1048 (1.0 KiB) TX bytes:8560 (8.3 KiB)

[root@Server ~]#
```

#dhclient eth0

How to assign IP address in Linux

ifconfig command can be used to assign the IP address but as I said above during the exam we should use best available command. Use **system-config-network** command to assign IP address.

#system-config-network

```
root@Server
File Edit View Search Terminal Help
[root@Server ~]# system-config-network
```

How to restart network service

Whenever you made change in IP configuration, you have to restart the network service so change can be applied. To restart network service run following command

```
#service network restart
```

How to start network service

During the exam you may get a system with network service disabled. To check network service run following command.

```
root@Server:~
File Edit View Search Terminal Help
[root@Server ~]# chkconfig --list network
network          0:off    1:off    2:off    3:off    4:off    5:off    6:off
[root@Server ~]#
```

if network service is off, run following command to on it.

```
root@Server:~
File Edit View Search Terminal Help
[root@Server ~]# chkconfig --list network
network          0:off    1:off    2:off    3:off    4:off    5:off    6:off
[root@Server ~]# chkconfig network on
[root@Server ~]# chkconfig --list network
network          0:off    1:off    2:on     3:on     4:on     5:on     6:off
[root@Server ~]#
```

Network Configuration Files

Services in Linux are managed through the several configuration files. In this article we will walk through the network configuration files.

This article is the part of article series. Previous articles of this series.

IP address

[How to assign IP address in Linux](#)

[Networking tools](#)

From previous articles you have learned the basic of IP address and their associated commands. In this article we addressing associated configuration files.

This article is written for RHCE exam prospective so we are including simplified configuration files.



These configuration files determine whether networking is started during the system boot process or not. Check these files when you have trouble with network configuration in Exam.

- /etc/init.d/network
- /etc/sysconfig/network
- /etc/sysconfig/network-scripts
- /etc/sysconfig/network-scripts/ifcfg-eth0
- /etc/nsswitch.conf
- /etc/hosts
- /etc/resolv.conf

/etc/init.d/network

/etc/init.d directory store script files. You can run the scripts directly, or use the service command to start/stop. We will demonstrate both.

Sometimes by mistake you may deactivate the network interface. Or there is an unknown error in configuration. In trouble this should be first point to check.

Execute script directly

```
# /etc/init.d/network status
root@Server:~#
File Edit View Search Terminal Help
[root@Server ~]# /etc/init.d/network status
Configured devices:
lo eth0
Currently active devices:
lo eth0
[root@Server ~]#
```

Use service command to execute script

```
#service network status
```

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# /etc/init.d/network status  
Configured devices:  
lo eth0  
Currently active devices:  
lo eth0  
[root@Server ~]# service network status  
Configured devices:  
lo eth0  
Currently active devices:  
lo eth0  
[root@Server ~]#
```

Output will be same in both case it should list configured and active devices. Output will give you a clue for future steps. If a main device such as eth0 is not listed as active, that explains why the network seems to be down. Try to restart the network service.

```
#service network restart  
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# service network restart  
Shutting down interface eth0: Error: Device 'eth0' (/org/freedesktop/NetworkManager/Devices/0) disconnecting failed: This device is not active [FAILED]  
Shutting down loopback interface: [ OK ]  
Bringing up loopback interface: [ OK ]  
[root@Server ~]#
```

Any change made in IP configuration will not take place until you restart the network interface. This script will restart the network interface.

```
#/etc/init.d/network restart  
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# /etc/init.d/network restart  
Shutting down interface eth0: Error: Device 'eth0' (/org/freedesktop/NetworkManager/Devices/0) disconnecting failed: This device is not active [FAILED]  
Shutting down loopback interface: [ OK ]  
Bringing up loopback interface: [ OK ]  
[root@Server ~]#
```

If a restart of networking services does not solve the issue move to the next steps. Next step is to get into the configuration files.

/etc/sysconfig/network

This file contains global configuration settings.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# cat /etc/sysconfig/network  
NETWORKING=yes  
HOSTNAME=Server  
[root@Server ~]#
```

This file specifies routing and host information for all network interfaces.

It is used to contain directives which are to have global effect and not to be interface specific.

Directive that you should check here for is NETWORKING=[yes][no].

If directive NETWORKING is set to no then the /etc/init.d/network script doesn't activate any network devices. It must be set to yes in order to start networking.

Directive HOSTNAME controls computer name. If you want to change computer name, change it here.

If networking still not start check the status of networking service.

If the settings next to runlevels 3 and 5 are off, that's a problem.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# chkconfig --list network  
network      0:off  1:off  2:off  3:off  4:off  5:off  6:off  
[root@Server ~]#
```

To make sure a service is active in appropriate runlevels, run the chkconfig network on command.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# chkconfig --list network  
network      0:off  1:off  2:off  3:off  4:off  5:off  6:off  
[root@Server ~]# chkconfig network on  
[root@Server ~]# chkconfig --list network  
network      0:off  1:off  2:on   3:on   4:on   5:on   6:off  
[root@Server ~]#
```

/etc/sysconfig/network-scripts

/etc/sysconfig/network-scripts directory contain executable files based on a series of text commands. These executable files are actually scripts based on the ifup and ifdown commands customized for the network device type.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# ls /etc/sysconfig/network-scripts/  
ifcfg-eth0  ifdown-isdn  ifup-aliases  ifup-plusb  
ifcfg-lo   ifdown-post  ifup-bnep   ifup-post  
ifdown    ifdown-ppp   ifup-eth    ifup-ppp  
ifdown-bnep  ifdown-routes  ifup-ippp  ifup-routes  
ifdown-eth   ifdown-sit   ifup-ipv6  ifup-sit  
ifdown-ippp  ifdown-tunnel  ifup-isdn  ifup-tunnel  
ifdown-ipv6  ifup        ifup-plip  ifup-wireless  
[root@Server ~]#
```

service network restart command may return with error like it in above example for eth0. In such a situation you should try to reactivate particular network device with ifup or ifdown command.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# ifdown eth0  
Error: Device 'eth0' (/org/freedesktop/NetworkManager/Devices/0) disconnecting failed: This device is not active  
[root@Server ~]# ifup eth0  
Active connection state: activating  
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/11  
state: activated  
Connection activated  
[root@Server ~]#
```

/etc/sysconfig/network-scripts/ifcfg-eth0

This file contain configuration for eth0 first network adaptor. What you see in the ifcfg-eth0 file depends on how that first Ethernet network adapter was configured.

```
root@Server:~ 
File Edit View Search Terminal Help
[root@Server ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
NM_CONTROLLED=yes
ONBOOT=no
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME="System eth0"
UUID=5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
USERCTL=no
HWADDR=00:0C:29:6F:D9:13
PEERDNS=yes
PEERROUTES=yes
[root@Server ~]#
```

For exam you should understand following directive

DEVICE	Type of device. for example lo=loopback adaptor, eth0= first Ethernet, eth1 second Ethernet etc.
IPADDR	Static IP Address
NETMASK	Network mask or subnet mask
NETWORK	Network ID or network address
BROADCAST	Broadcast address
GATEWAY	IP address of the default gateway
ONBOOT	specify whether the device is activated during the boot process
NAME	common name for the device
HWADDR	hardware address of network interface also known as MAC address
NM_CONTROLLED	Specify that network card should be controlled by the Network Manager service or not. If it is set to yes be sure that Network Manager running
BOOTPROTO	How IP address would be configured. dhcp for dynamic configuration, static for static ip configuration

/etc/nsswitch.conf

This file includes database search entries. It include from authentication to name services.

```
root@Server:~  
File Edit View Search Terminal Help  
#  
# /etc/nsswitch.conf  
#  
# An example Name Service Switch config file. This file should be  
# sorted with the most-used services at the beginning.  
#
```

It includes the following entry which determines what database is search first.

```
root@Server:~  
File Edit View Search Terminal Help  
hosts: files dns  
  
# Example - obey only what nisplus tells us...  
#services: nisplus [NOTFOUND=return] files  
#networks: nisplus [NOTFOUND=return] files  
#protocols: nisplus [NOTFOUND=return] files  
#rpc: nisplus [NOTFOUND=return] files  
#ethers: nisplus [NOTFOUND=return] files  
#netmasks: nisplus [NOTFOUND=return] files  
  
bootparams: nisplus [NOTFOUND=return] files  
  
ethers: files  
netmasks: files  
networks: files  
protocols: files  
rpc: files  
services: files  
  
netgroup: nisplus  
publickey: nisplus  
  
automount: files nisplus  
aliases: files nisplus  
  
[root@Server ~]#
```

When a system gets a request to search for a hostname, the preceding directive means the /etc/hosts file is searched first.

If that name is not found in /etc/hosts, the next step is to search available configured DNS servers, normally using that configured in the /etc/resolv.conf file.

/etc/hosts

This file is used to resolve hostnames that cannot be resolved any other way. It can also be used to resolve hostnames on small networks with no DNS server.

This file by default contains a line specifying the IP address of the loopback device (127.0.0.1) as localhost.localdomain.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# cat /etc/hosts  
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4  
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6  
[root@Server ~]#
```

/etc/resolv.conf

This file specifies the IP addresses of DNS servers and the search domain. Unless configured to do otherwise, the network initialization scripts populate this file.

```
root@Server:~  
File Edit View Search Terminal Help  
[root@Server ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
  
# No nameservers found; try putting DNS servers into your  
# ifcfg files in /etc/sysconfig/network-scripts like so:  
#  
# DNS1=xxx.xxx.xxx.xxx  
# DNS2=xxx.xxx.xxx.xxx  
# DOMAIN=lab.foo.com bar.foo.com  
[root@Server ~]#
```

These are the files which you need to be familiar with. So go through these files again and again until you feel comfortable.

How to configure FTP server in RHEL 7

Your will configure FTP Server on RHEL7. FTP is the most widely used protocol for file transfer. As a linux Administrator you

should know

- FTP stand for File Transfer Protocol.
- FTP does not require to login directly into the remote host
- FTP transfer data without encryption
- vsftpd is the only stand-alone FTP distributed With RHEL 7
- vsftpd stand for Very Secure FTP Daemon
- vsftpd is secure, fast and stable version of FTP
- vsftpd efficiently handle large numbers of connection securely
- You should use SFTP instead of FTP while transferring data over public network like Internet

Configure FTP Server on RHEL 7:-

vsftpd package is required for FTP Server. Check whether package is installed or not.

If package is missing install it first.

Step 1:-

```
[root@localhost ~]# rpm -q vsftpd    # If not installed then installed it using yum
```

```
[root@localhost ~]# yum install vsftpd
```

Step 2: Configure vsftpd service to start

```
[root@localhost ~]# systemctl restart vsftpd
```

Configure vsftpd service to start at boot:-

```
[root@localhost ~]# systemctl enable vsftpd
```

4. Manage the firewall

FTP Server is by default configured to listen on port 21. Port 21 must be opened if you have configured firewall. The configuration of a firewall for an FTP server is a relatively simple process

```
[root@localhost xinetd.d]# firewall-cmd --add-port=21/tcp
```

OR



```
[root@localhost xinetd.d]# firewall-cmd --add-service=ftp
```

Go on Server system and open main ftp configuration file **/etc/vsftpd/vsftpd.conf**

FTP non-anonymous server

In this exercise we will configure FTP server that allow local users logins to their home directories. Download/upload must be allowed for these users. Go on server system and open **/etc/vsftpd/vsftpd.conf** file

Comment **anonymous_login=YES**, uncomment **local_enable** and save the file

Enable anonymous user to upload file:

Uncomment the line **anon_other_write_enable = yes**

And

Chmod **o+w /var/ftp/pub**

open **/etc/vsftpd/user_list** file

Users listed on **/etc/vsftpd/user_list** are not allowed to login on FTP server. Add user **vikarm** in it. This file also have an entry for root user that why root user is denied from FTP login. If you want to enable root user for ftp session just remove its entry from this file [Enable root for FTP session is not recommended in any circumstances, change at your own risk.

Important: by default root user is not allowed to login via ftp

To login via root remove name of root from two file .

1. First is **/etc/vsftpd/ftpuser**
2. Second **/etc/vsftpd/user_list**

Configure FTP client on RHEL7

```
[root@localhost ~]# yum install ftp
```

To connect with server you can use ftp command:

```
[root@redhat7 ~]# ftp 127.0.0.1
```

Connected to 127.0.0.1 (127.0.0.1)



220 (vsFTPd 3.0.2)

Name (127.0.0.1:root): ftp

331

Please specify the password.

Password:

230 Login successful.

OR

USE graphical method like web browser and filezilla software



How to configure SSH Server in RHEL 7

SSH server also used to login remotely but having no security issue to configure SSH server and SSH client in RHEL7.

RHCE 7 configured as below

- Configure key-based SSH authentication.

- Configure additional SSH options described in documentation.

As a Linux administrator you should know

- SSH stand for Secure Shell.
- SSH is a network protocol for secure data communication.
- SSH protocol allows remote command line login.
- SSH protocol enables remote command execution.
- To use SSH you need to deploy SSH Server and SSH Client program respectively.
- OpenSSH is a FREE version of the SSH.
- Telnet, rlogin, and ftp transmit unencrypted data over internet.
- OpenSSH encrypt data before sending it over insecure network like internet.
- OpenSSH effectively eliminate eavesdropping, connection hijacking, and other attacks.
- OpenSSH provides secure tunneling and several authentication methods.
- OpenSSH replace Telnet and rlogin with SSH, rcp with scp, ftp with sftp.

SSH Tools

sshd

The daemon service that implements the ssh server. By default it must be listening on port 22 TCP/IP.

ssh

The ssh [Secure Shell command] is a secure way to log and execute commands in to SSH Server system.

scp

The Secure Copy command is a secure way to transfer files between computers using the private/public key encryption method.

ssh-keygen

This utility is used to create the public/private keys.

ssh-agent

This utility holds private keys used for RSA authentication.

ssh-add

Adds RSA identities to the authentication agent ssh-agent.

On your laptop or Desktop

- Configure a SSH server and SSH client on RHEL7.
- Create two user **user1** and **user2** and verify that both users can login in SSH server from SSH client.
- Do not allow **root** and **user1** users to login to it and allow the rest of users. To confirm it login from **user2**.
- Re-configure SSH Server to allow login only using public / private keys. Generate keys for **user2** and verify that **user2** can login using keys

How to configure SSH Server in RHEL 7

Two RPM are required to configure and run OpenSSH server.

- openssh-server
- openssh

Before you start configuration make sure that you have necessary RPM packages installed. Install if any RPM is missing.

```
[root@localhost ~]# rpm -q openssh-server
```

```
openssh-server-6.4p1-8.el7.x86_64
```

Check the current status of **sshd** service, it must be running. If service is stopped start it. Options you need with service command are **start | stop | restart | status**

```
[root@localhost xinetd.d]# systemctl status sshd
```

```
[root@localhost xinetd.d]# systemctl restart sshd
```

Note: To make to persistant after reboot use below command

```
[root@localhost xinetd.d]# systemctl enable sshd
```

Important : If during making connection if there is any connectivity issue then add a firewall rule

```
[root@localhost xinetd.d]# firewall-cmd --add-port=22/tcp
```

OR

```
[root@localhost xinetd.d]# firewall-cmd --add-service=ssh
```

Note: For the making any changes in configuration file which is (sshd_config)

```
[root@localhost ~]# cd /etc/ssh/
```

```
[root@localhost ssh]# ls
```

```
moduli      sshd_config      ssh_host_ecdsa_key.pub ssh_host_rsa_key.pub
```

To allow or deny users and some other configuration using ssh:

```
[root@localhost ~]# vim sshd_config  
# on line 42: uncomment and change the value to 'no'
```

```
PermitRootLogin no
```

```
# on line 65: uncomment the following
```

```
PermitEmptyPasswords no  
PasswordAuthentication yes  
Save & quit then execute the following command.
```

```
# at any line
Allowusers user1 user2      ## these users only able to login via ssh
denysers user1 user2        ## these users are not able to login via ssh

[root@localhost xinetd.d]# systemctl restart sshd
```

How to configure SSH client on RHEL 7:

openssh-clients rpm is required for ssh client.

Check necessary RPM, install if any missing

```
[root@localhost ~]# rpm -q openssh-clients
openssh-clients-6.4p1-8.el7.x86_64
```

Go back on **linuxclient** system and verify that we have **user1** and **root**. Also verify that **user1** and **root** able to login in SSH server

```
[root@localhost ~]# ssh user1@192.168.0.12
```

Web Server

When you view a web page over the Internet, the code to create that page must be retrieved from a server somewhere on the Internet. The server that sends your web browser the code to display a web page is called a web server. There are countless web servers all over the Internet serving countless websites to people all over the world. Whether you need a web server to host a website on the Internet a Red Hat Enterprise Linux server can function as a web server using the **Apache HTTP server**. The Apache HTTP server is a popular, open source server application that runs on many UNIX-based systems as well as Microsoft Windows.

Example 1. There are two sites www.vinita.com and www.nikita.com. Both sites are mappings to 192.168.0.X IP address where X is your Host address. Configure the Apache web server for these sites to make accessible on web

Configure web server.

In this example we will configure a **web server**.

necessary rpm for web server is **httpd**, **httpd-devel** check them for install



Step 1. check for software is installed or not:

```
[root@localhost ~]# rpm -q httpd  
[root@localhost ~]# rpm -q httpd-devel
```

For Installing

```
[root@localhost ~]# yum install httpd httpd-devel
```

Now configure the ip address to **192.168.0.12** and check it

Step 2:

start **httpd daemons** and verify its running **status**

```
[root@localhost ~]# systemctl restart httpd
```

Also enable the firewall rule

```
[root@localhost ~]# firewall-cmd --add-port=80/tcp  
[root@localhost ~]# firewall-cmd --add-service=http
```

Step 3:

Now there are some configuration which are already configured and for extra configuration

1. By default documentroot is /var/www/html/
2. Page name is index.html

for testing purpose we are writing **site name** in its **index page**

```
[root@localhost ~]# cd /var/www/html/
```

```
echo hi >index.html
```

Note: after doing above step you can test via web browser by entering IP or hostname of web server

Configure virtual hosting:

In this example we will host a website **www.vinita.com** to apache web server. Create a **documents root** directory for this website and a **index page**

now open **/etc/hosts** file

in the **end of file** bind system ip with www.vinita.com

```
[root@localhost ~]# vim /etc/hosts
```

```
127.0.0.1 www.vinita.com
```

now open **/etc/httpd/conf/httpd.conf** main configuration file of **apache server**

```
[root@localhost ~]# vim /etc/httpd/conf/httpd.conf
```

```
NameVirtualHost 192.168.0.12:80
```



Now go in the end of file and copy last seven line [virtual host tag] and paste them in the end of file.

```
<virtualhost 192.168.0.12:80>
```

```
Documentroot /var/www/html/
```

```
Servername www.vinita.com
```

```
</virtualhost>
```

```
<virtualhost 192.168.0.12:80>
```

```
Documentroot /var/www/virtual/
```

```
Servername www.myhome.com
```

```
</virtualhost>
```

```
[root@localhost ~]# mkdir /var/www/virtual
```

```
[root@localhost ~]# echo "hello" >index.html
```

Note: if you want any security in any documentroot then inside virtualhost

```
<virtualhost 192.168.0.12:80>
```

```
Documentroot /var/www/virtual
```

```
Servername www.myhome.com
```

```
<directory /var/www/virtual/>
```

```
Order allow,deny
```

```
Allow from 127.0.0.1 192.168.0.0/24
```

```
</virtualhost>
```



Important:

you have done necessary configuration now restart the httpd service:

```
[root@localhost ~]# systemctl restart httpd
```

Apache clients:

Important: you can use web browser for apache client to test your web page



NFS Server

NFS, or **Network File System**, is a server-client protocol for sharing files between computers on a common network. NFS enables you to mount a file system on a remote computer as if it were local to your own system. You can then directly access any of the files on that remote file system. The server and client do not have to use the same operating system. The client system just needs to be running an **NFS client** compatible with the **NFS server**.

For example **NFS server** could be a Linux system and Unix could be a client. But it can't be a window system because window is not NFS compatible. The NFS server exports one or more directories to the client systems, and the client systems mount one or more of the shared directories to local directories called mount points. After the share is mounted, all I/O operations are written back to the server, and all clients notice the change as if it occurred on the local filesystem.

A manual refresh is not needed because the client accesses the remote filesystem as if it were local.because access is granted by IP address, a username and password are not required. However, there are security risks to consider because the **NFS server** knows nothing about the users on the client system.

Example 1 Some users home directory is shared from your system. Using **showmount -e** localhost command, the shared directory is not shown. Make access the shared users home directory

Example 2 The System you are using is for **NFS (Network File Services)**. Some important data are shared from your system. Make automatically start the nfs and portmap services at boot time



Example 3 Share **/data** directory using NFS only to **192.168.0.0/24** members. These hosts should get read and write access on shared directory.

Configure nfs server

In this example we will configure a nfs server and will mount shared directory from client side.

For this example we are using two systems one linux server one linux clients . To complete these per quest of nfs server Follow this link

Network configuration in Linux

- A linux server with ip address 192.168.0.254 and hostname Server
- A linux client with ip address 192.168.0.1 and hostname Client1
- Updated /etc/hosts file on both linux system
- Running portmap service

Step 1: Check the required rpm and if not installed then install it

```
[root@localhost ~]# rpm -q nfs-utils # If not installed then installed it
```

OR

```
[root@redhat7~] yum install nfs-utils
```

Step 2: configure nfs server

now create a **/data** directory and grant full permission to it

now open **/etc/exports** file

share **data** folder for the network of **192.168.0.254/24** with read and write access

```
/data 192.168.0.0/24(sync,rw)
```

Step 3: start or restart the service

```
[root@localhost ~]# systemctl enable nfs
```

```
[root@localhost ~]# systemctl restart nfs
```



Note: also restart **nfs daemons** with **exportfs**

```
[root@localhost ~]# exportfs -r
```

configure client system:

ping from **nfs server** and then check the **share folder** by **using showmount command**

```
[root@localhost ~]# showmount -e 192.168.0.12 ## (here 192.168.0.12 is server IP )
```

now **mount** this share folder on **mnt** mount point. To test this share folder change directory to **mnt** and create a **test file**

```
[root@localhost ~]# mount -t nfs 192.168.0.12:/data /mnt
```

After use you should always **umount** from **mnt** mount point

```
[root@localhost ~]# umount /mnt
```

NIS Server

NIS, or **Network Information Systems**, is a network service that allows authentication and login information to be stored on a centrally located server. This includes the username and password database for login authentication, database of user groups, and the locations of home directories.

RHCE exam questions

One **NIS Domain** named **rhce** is configured in your lab, server is **192.168.0.254**. nis1, nis2,nis3 user are created on domain server. Make your system as a member of **rhce** domain. Make sure that when nis user login in your system home directory should get by them. Home directory is shared on server **/rhome/nis1**.

RHCE exam doesn't ask candidate to configure NIS server. It test only NIS client side configuration. As you can see in example questions. But here in this article we will configure both server and client side for testing purpose so you can get more depth knowledge of nis server

Configure NIS server

In this example we will configure a NIS server and a user nis1 will login from client side.

For this example we are using two systems one linux server one linux clients . To complete these per quest of nis server Follow this link

Network configuration in Linux

- A linux server with ip address 192.168.0.254 and hostname Server
- A linux client with ip address 192.168.0.1 and hostname Client1
- Updated /etc/hosts file on both linux system
- Running portmap service
- Firewall should be off on server

We suggest you to review that article before start configuration of nis server. Once you have completed the necessary steps follow this guide.

Seven rpm are required to configure nis server. **ypserv, cach, nfs, make, ypbnd, portmap** check them if not found then install

```
[root@localhost ~]# rpm -q ypbnd  
[root@localhost ~]# rpm -q rpcbind  
[root@localhost ~]# rpm -q ypserv
```

Configure Nis server:-

Step 1:

```
[root@localhost ssh]# yum install ypserv
```

Step 2:- assign a domain-name to Nis server using below method

```
[root@localhost ssh]# ypdomainname lw
```

Note: you can use existing username or can create your own

```
[root@localhost ssh]# useradd vimal  
[root@localhost ssh]# passwd vimal  
[root@localhost ssh]# cd /var/yp  
[root@localhost ssh]# make
```

Note: During make command if there is any error like rpcbind is not registered then do the step third first

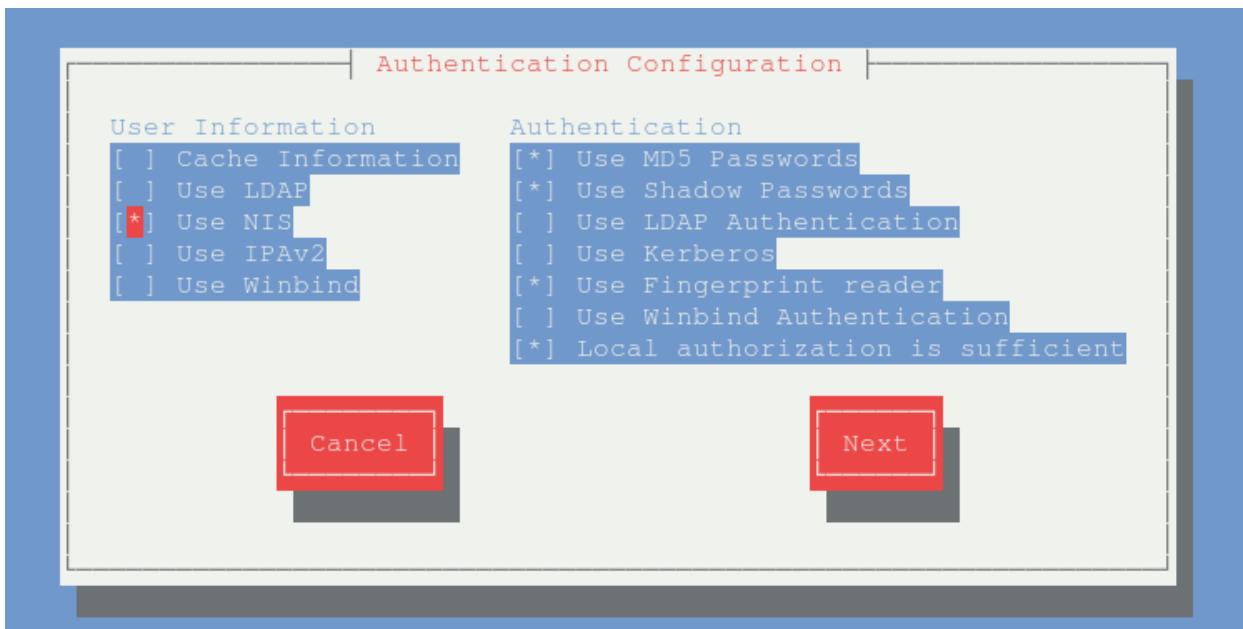
Step : 3 now start or restart the service of ypserv

```
[root@localhost ssh]# systemctl restart ypserv
```

Configure NIS Client:-

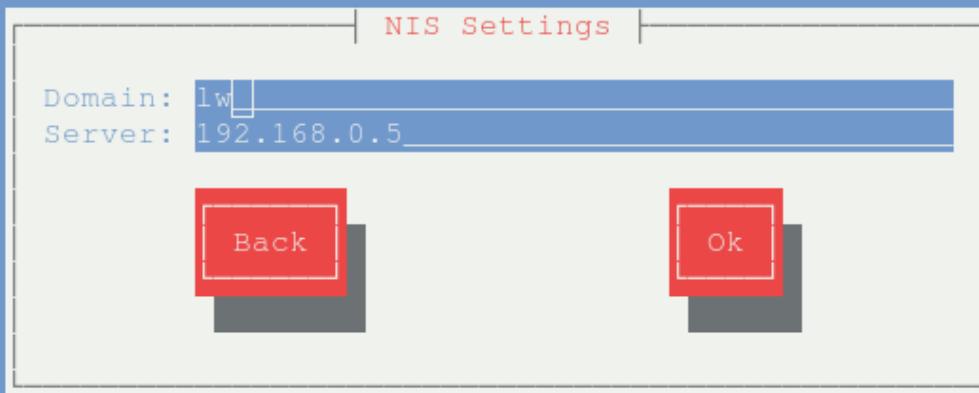
For nis client you have to install yplibd package first and use below steps to use nis

```
[root@localhost ssh]# yum install yplibd
[root@localhost ssh]# authconfig-tui      # when you fire this command it will result like this
```



Click on Use Nis using space button and press next button as shown in above figure and made some entry as show below figure

Note: In below figure domain is the same which was assigned in NIS server and IP address of server



NOTE: now you can login via any user which are created in NIS server via command line or graphical

```
[root@localhost ssh]# su - vimal
```

Configure Samba Server

Most Linux systems are the part of networks that also run Windows systems. Using Linux **Samba servers**, your Linux and Windows systems can share directories and printers. This is most use full situation where your clients are window native and you want to use the linux security features.

There are mixed System running on Linux and Windows OS. Some users are working on Windows Operating System. There is a **/data** directory on linux server should make available on windows to only vinita should have right to connect with samba server . Configure to make available

Configure samba server:

In this example we will configure a **samba** server and will transfer files from client side. For this example we are using two systems one linux server one window clients.

- A linux server with ip address 192.168.0.254 and hostname Server
- A window client with ip address 192.168.0.2 and hostname Client2
- Updated /etc/hosts file on linux system
- Running portmap and xinetd services

- Firewall should be off on server

We have configured all these steps in our previous article.

We suggest you to review that article before start configuration of samba server. Once you have completed the necessary steps follow this guide.

Step 1:

samba rpm is required to configure samba server. check them if not found then install

```
[root@localhost ~]# rpm -q samba
```

OR

```
[root@localhost ~]# rpm -qa samba*
```

For installing packages:

```
[root@localhost ~]# yum install samba
```

Step 2:

Create a normal user named **Vinita**

```
[root@localhost ~]# useradd Vinita
```

now create **/data** directory and grant it **full permission**

```
[root@localhost ~]#mkdir /data
```

```
[root@localhost ~]#chmod 777 /data
```

open **/etc/samba/smb.conf** main samba configuration files

```
[root@localhost ~]# vim /etc/samba/smb.conf
```

our task is to share **data** folder for **vinita** user so go in the end of file and do editing as shown here

[sharename]

Path = **/data**

Hosts allow = **192.168.0.0/24**

Valid users = **Vinita**



Public = no

Writable = no

Now save the file

Finally Now add vinita user to **samba user**

```
[root@localhost ~]# smbpasswd -a Vinita
```

Step 3. start the service of smb

```
[root@localhost ~]#systemctl restart smb
```

```
[root@localhost ~]#systemctl enable smb
```



ISO 9001:2008 CERTIFIED ORGANISATION

Client configuration for samba server:

Case 1 . In client is linux then install cifs-utils package if not installed and use below method to access

```
[root@localhost ~]#smbclient -U vinita //192.168.0.12/sharename
```

Note: Furthur you can use the same method like in ftp server to download and upload command like get and put

Case: 2 If client is windows then go to run type \192.168.0.12 (here ip is server ip)

DHCP SERVER in RHEL 7:

For assigning IP address there are two methods

1. Static method
2. Dynamic method

Today we are talking about dynamic method of IP address allocation

DHCP: - dhcp is a protocol for assigning IP address to computer system, mobile phones, router etc by dynamic method OR we can say every device which requires IP address.

DHCP:-stands for “Dynamic Host Configuration protocol “

Configuring dhcp server in Redhat 7

Important: - As you all know that we use three steps for making a server.

Step 1:- check the required software and install it if not installed by using below given steps

```
[root@localhost ~]# rpm -q dhcp      # Here rpm command for checking dhcp package
```

Dhcp is not installed

```
[root@redhat7 Desktop]# yum install dhcp
```

Step 2: configure the dhcp server using configuration file

```
[root@redhat7 Desktop]# cd /etc/dhcp/
```

```
[root@redhat7 dhcp]# ls
```

```
dhclient.d  dhcpd6.conf  dhcpd.conf
```



Note: here `dhcpd.conf` is the main configuration file for dhcp server when you open the file some instruction are given use them if you required or use below configuration steps

For copying manual file you can use below given `cp` command

```
[root@redhat7 dhcp]# cp /usr/share/doc/dhcp4-2.1/dhcpd.conf.sample /etc/dhcp/dhcpd.conf
```

OR

Write done necessary configuration

```
[root@redhat7 dhcp]# vim dhcpd.conf
```

```
default-lease-time 600;
```



max-lease-time 7200;

```
subnet 20.0.0.0 netmask 255.0.0.0 {
```

```
range 20.0.0.10 20.0.0.100;
```

```
}
```

Note: To fix IP of every computer system which is allocated by dhcp you have to bind every system with their mac(physical address)

```
host redhat71 {
```

```
hardware ethernet 08:00:07:26:c0:a5;
```

```
fixed-address 20.0.0.50;
```

```
}
```

```
host redhat61 {
```

```
hardware ethernet 20:CF:30:F3:EB:14;
```

```
fixed-address 20.0.0.51;
```

```
}
```

Step 3: start or restart the service of dhcp

```
[root@redhat7 dhcp]# systemctl restart dhcpcd
```

Important:- To make dhcp service persistant after rebooting your server use below command like in redhat version 6 we use (chkconfig dhcp on)

```
[root@redhat7 dhcp]# systemctl enable dhcpcd
```

Important:- If during ip allocation for clients if there is any problem then add a firewall rule for dhcp server port:

Dhcp server port: 67

Dhcp Client port : 68





```
[root@redhat7 dhcp]# firewall-cmd --add-port=67/udp
```

OR

```
[root@redhat7 dhcp]# firewall-cmd --add-service=dhcp
```

Now your dhcp server ready to use.

Dhcp client configuration:-

For dhcp client there is a command known as **dhclient** by using this command you can assign IP address to your system use given method.

```
[root@redhat7 ~]# dhclient -v enp2s0
Internet Systems Consortium DHCP Client 4.2.5
Copyright 2004-2013 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
```

```
Listening on LPF/enp2s0/20:cf:30:f2:f4:02
Sending on LPF/enp2s0/20:cf:30:f2:f4:02
Sending on Socket/fallback
DHCPDISCOVER on enp2s0 to 255.255.255.255 port 67 interval 6 (xid=0x2807414d)
DHCPREQUEST on enp2s0 to 255.255.255.255 port 67 (xid=0x2807414d)
DHCPoffer from 20.0.0.2
DHCPACK from 20.0.0.2 (xid=0x2807414d)
bound to 20.0.0.13 -- renewal in 281 seconds.
[root@redhat7 ~]# 
```

Configuring Kickstart automation In Redhat 7

Kickstart is the method where your install of O.S is Install automatically so for making kickstart file you need to follow these steps as given below.

Step 1: Select Installation method out of DVD/FTP/NFS/HTTP

I am selecting FTP for which is a type of network installation :-

- Install FTP server and Copy DVD's content to FTP home directory as given below

```
[root@redhat7 lw_tips]# yum install vsftpd -y
[root@redhat7 lw_tips]# cd /var/ftp/
[root@redhat7 lw_tips]# cp -rvf DVD /var/ftp/
```

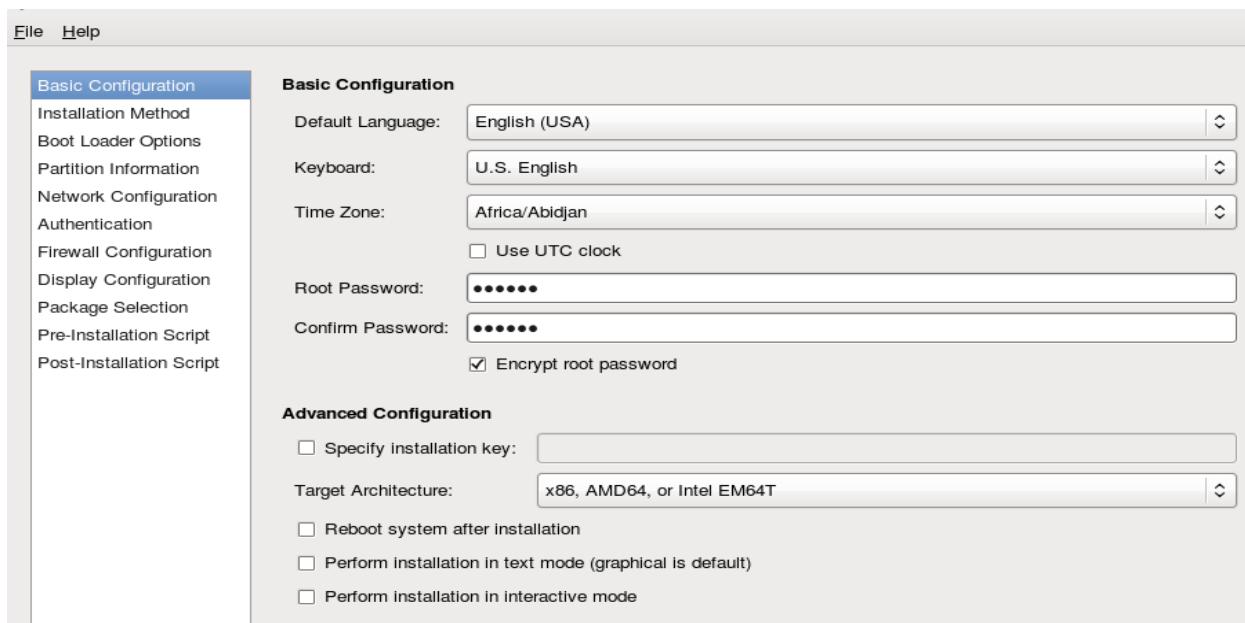
Note: here DVD is a folder where your all rhel 7 content is present so simply copy all the content to /var/ftp/

```
[root@redhat7 lw_tips]# systemctl restart vsftpd
[root@redhat7 lw_tips]# systemctl enable vsftpd
[root@redhat7 lw_tips]# firewall-cmd --add-service=ftp --permanent
[root@redhat7 lw_tips]# firewall-cmd --add-service=ftp
```

- Time For creating Kickstart file
 - [root@redhat7 lw_tips]# yum install system-config-kickstart
 - [root@redhat7 lw_tips]# system-config-kickstart

NOTE: Follow the screenshot given below

- Set the root password



- Set installation medium

[File](#) [Help](#)

Basic Configuration
Installation Method
Boot Loader Options
Partition Information
Network Configuration
Authentication
Firewall Configuration
Display Configuration
Package Selection
Pre-Installation Script
Post-Installation Script

Installation Method

- Perform new installation
 Upgrade an existing installation

Installation source

- | | | |
|--------------------------------------|---|---------------|
| <input type="radio"/> CD-ROM | FTP Server: | 192.168.1.254 |
| <input type="radio"/> NFS | FTP Directory: | DVD |
| <input checked="" type="radio"/> FTP | | |
| <input type="radio"/> HTTP | <input type="checkbox"/> Specify an FTP username and password | |
| <input type="radio"/> Hard Drive | FTP Username: | |
| | FTP Password: | |

3. Select and setup bootloader installation

[File](#) [Help](#)

Basic Configuration
Installation Method
Boot Loader Options
Partition Information
Network Configuration
Authentication
Firewall Configuration
Display Configuration
Package Selection
Pre-Installation Script
Post-Installation Script

Install Type

- Install new boot loader
 Do not install a boot loader
 Upgrade existing boot loader

GRUB Options

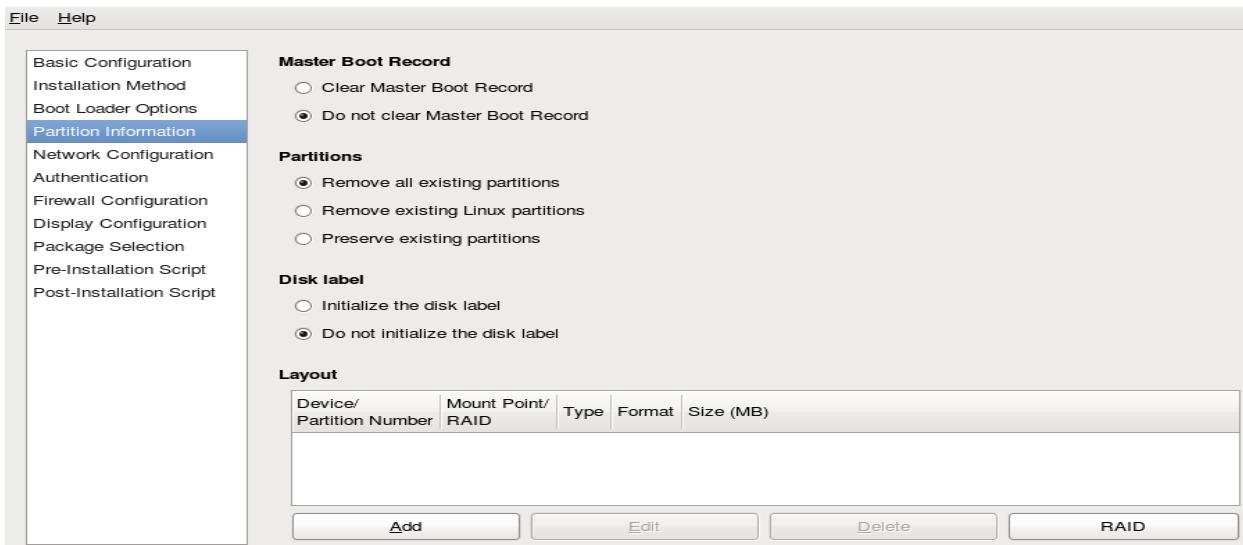
- Use GRUB password
 Password:
 Confirm Password:
 Encrypt GRUB password

Install Options

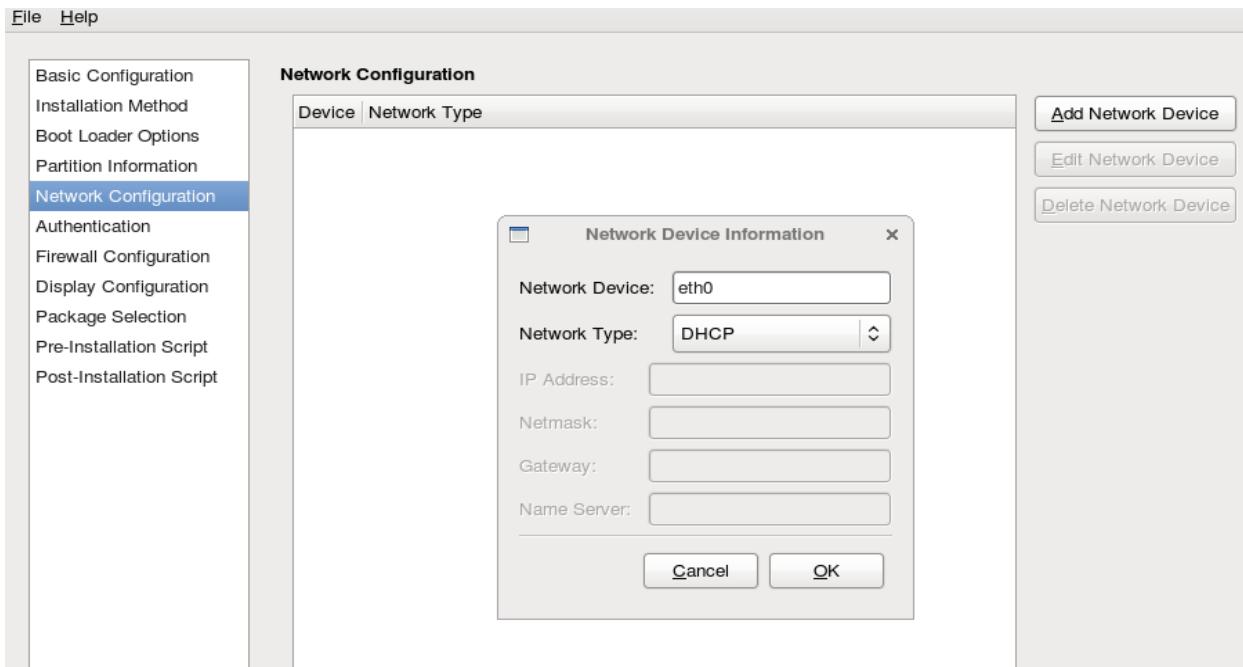
- Install boot loader on Master Boot Record (MBR)
 Install boot loader on first sector of the boot partition

 Kernel parameters:

Select partitions



4. Select network and ip address assign method



So by following below given steps you can configure kickstart installation method

Note: now you can save this file and put this to Installation media directory