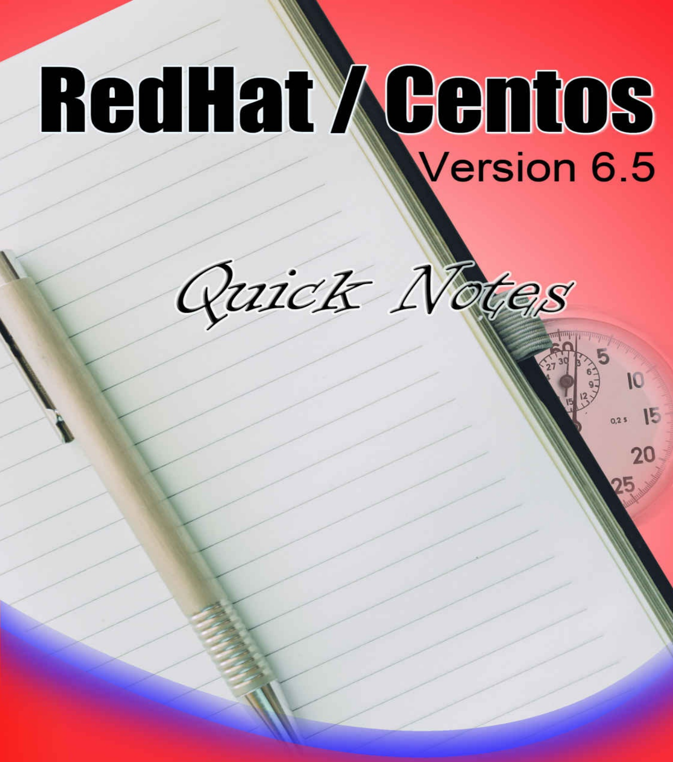
RedHat / Centos

Version 6.5

Quick Notes

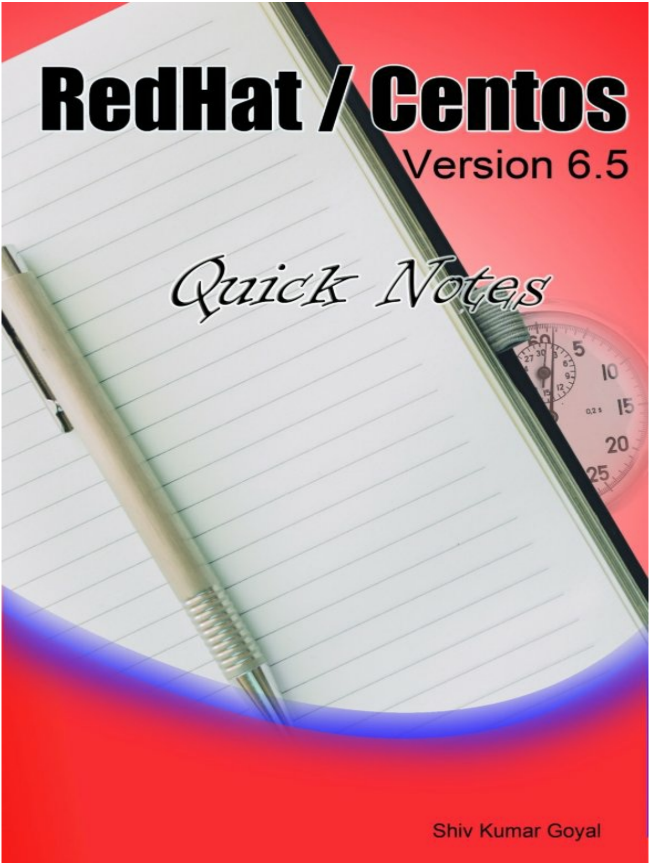


Shiv Kumar Goyal

RedHat / Centos

Version 6.5

Quick Notes



Shiv Kumar Goyal

RedHat and Centos Quick Notes

Shiv Kumar Goyal

Preface

This book is written keeping in mind Linux system administrators, who wants to learn Redhat/Centos but do not have time to read lot of books. This is book is excellent choice for preparing interview. I tried my level best to keep the text as precise as possible.

This book is specially prepared for

practical implementation of Redhat. I hope it will help the administrators in deploying Redhat in the production environment.

Thanks

Shiv Kumar Goyal

Contents

Chapter 1

Introduction

Linux is UNIX like Operating system. Linux is an open source project started by Linus Torvalds in 1991. There are thousands of Linux distributions in the market, but broadly can be classified on their root distribution for example Centos, Oracle and Scientific Linux based on Redhat, Debian based distributions like Ubuntu, Mint etc. The prominent player in free Linux are Ubuntu, Debian, Fedora, Opensuse etc. Redhat and SUSE is major player in non- free enterprise Linux distribution. Redhat and SUSE is RPM package based distribution where as Debian based distribution are of DEB packaging.

Fedora and Redhat

Fedora is free distribution and community project sponsored by Redhat. Fedora is upstream for Redhat enterprise Linux. Fedora is test bed for new features, which may get incorporate in upcoming Redhat Linux version. Main difference between the Fedora Linux and Redhat Enterprise Linux is support and life cycle of the product. Redhat is commercially supported product whereas Fedora is community supported. Redhat Enterprise Linux has life cycle of few years and supported up to 10 years but in case of Fedora new release come out after every 6 months and gets update for 13 months only. Redhat provides service level agreements, certification of hardware and software, which is important for enterprise organization.

Oracle Linux, Centos Linux and Scientific Linux distributions are derived from the sources of Red Hat Enterprise Linux. Provides same software as Redhat but without support from Redhat.

Chapter 2

Installation

The common two ways to install Redhat are:-

1. Interactive
2. Automated i.e. Kickstart

Interactive method

Interactive method can be either Text based or GUI.

Kickstart

For Kickstart installation, we have to create a single file containing the answers to all the questions Redhat installation normally asks during interactive installation. Once the installation starts, no user intervention is required.

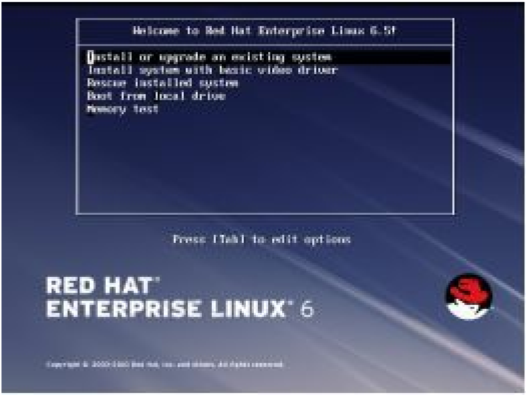
Steps to do Interactive installation

To start installation first download media from https://access.redhat.com/downloads.

Burn the downloaded ISO image file.

Start the system with first boot device as DVDROM.

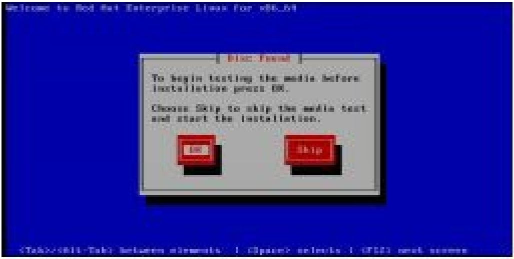
Once Installation menu comes, select install and upgrade an existing system.



Welcome to Red Hat Enterprise Linux 6.5!

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test
Press [Tab] to edit options
RED HAT ENTERPRISE LINUX 6

Select skip to test media.



Welcome to Red Hat Enterprise Linux for x86_64

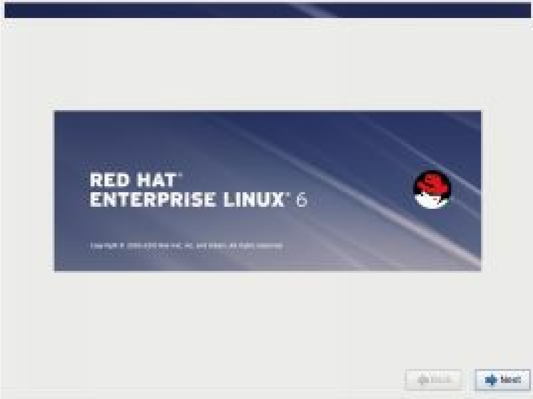
Disc Found

To begin testing the media before installation press OK.

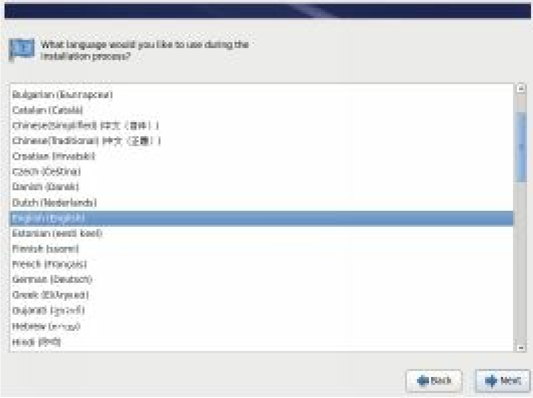
Choose Skip to skip the media test and start the installation.

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Press next.



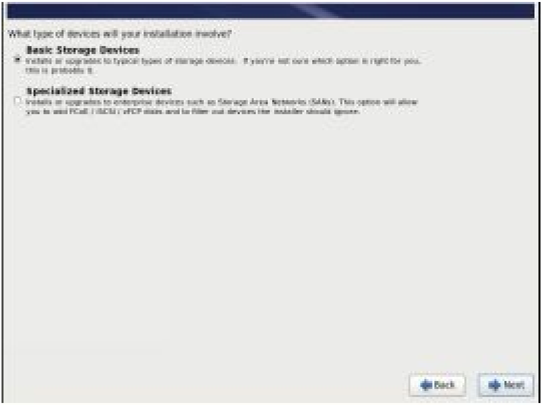
Select language and keyboard.



What language would you like to use during the installation process?

Bulgarian (Български)
Catalan (Català)
Chinese(Simplified) (中文（简体）)
Chinese(Traditional) (中文（正體）)
Croatian (Hrvatski)
Czech (Čeština)
Danish (Dansk)
Dutch (Nederlands)
English (English)
Estonian (eesti keel)
Finnish (suomi)
French (Français)
German (Deutsch)
Greek (Ελληνικά)
Gujarati (ગુજરાતી)
Hebrew (עברית)
Hindi (हिन्दी)

Select the storage.

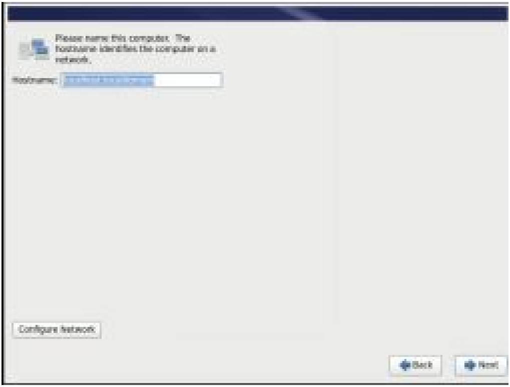


What type of devices will your installation involve?

● **Basic Storage Devices**
Installs or upgrades to typical types of storage devices. If you're not sure which option is right for you, this is probably it.

○ **Specialized Storage Devices**
Installs or upgrades to enterprise devices such as Storage Area Networks (SANs). This option will allow you to add FCoE / iSCSI / zFCP disks and to filter out devices the installer should ignore.

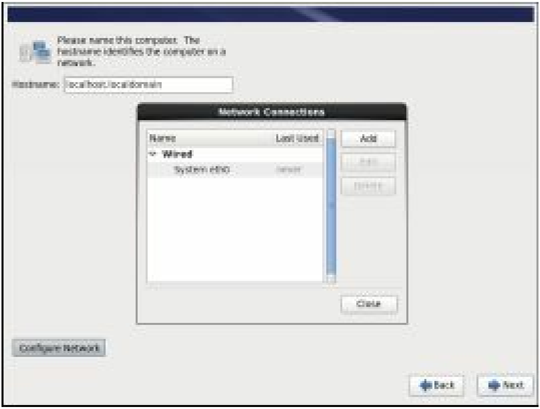
Write hostname.



Please name this computer. The hostname identifies the computer on a network.

Hostname:

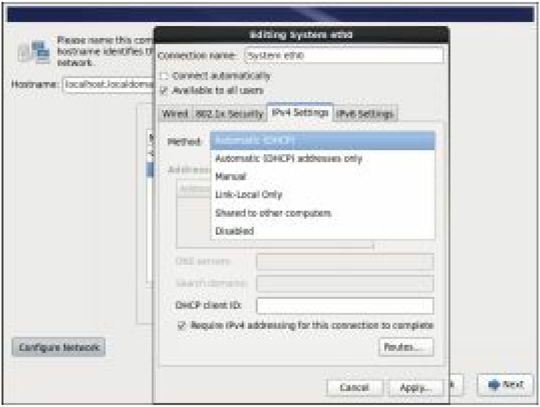
Click on configure network and select the network card.



Please name this computer. The hostname identifies the computer on a network.

Hostname: localhost.localdomain

. Select edit > select IP4 > Select method as manual from drop down menu if you have static IP address otherwise select Automatic.



Editing System eth0

Connection name: System eth0

□ Connect automatically

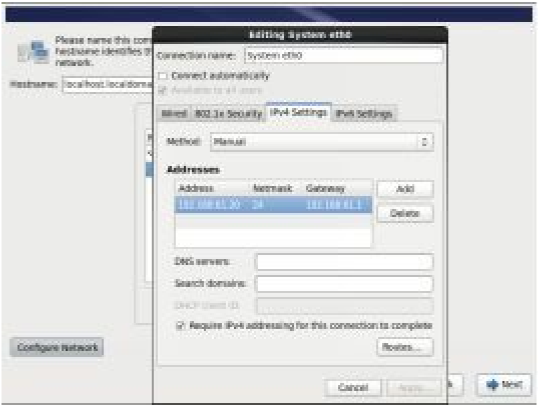
☑ Available to all users

Method: Automatic (DHCP)

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

- In case of static IP address, select add and provide IP address, Netmask, gateway and DNS server setting. Do not forget to click **connect automatically**.
- Then press Apply > close and next.



Hostname: localhost.localdoma

Connection name: System eth0

□ Connect automatically

☑ Available to all users

Method: Manual

Address	Netmask	Gateway
192.168.61.20	24	192.168.61.1

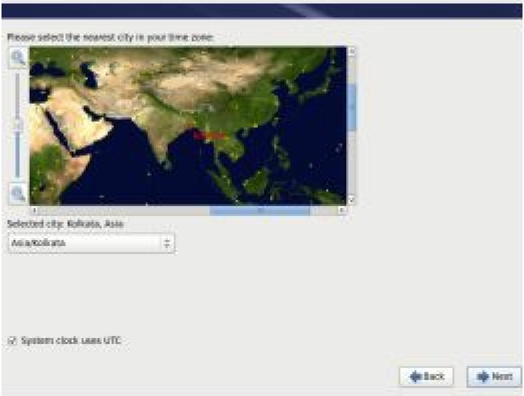
DNS servers:

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

. On the next screen, select time zone , Time zone is country specific so select the time zone accordingly



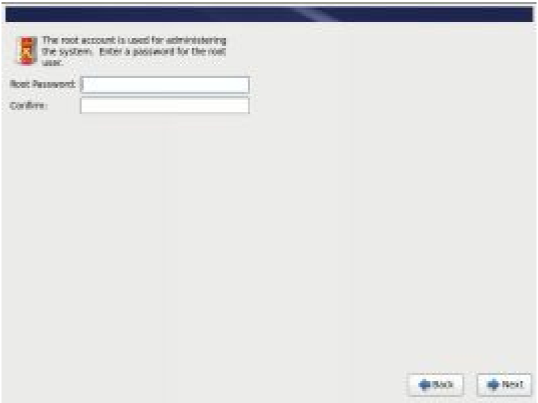
Please select the nearest city in your time zone:

Selected city: Kolkata, Asia

Asia/Kolkata

☑ System clock uses UTC

. Provide root password.

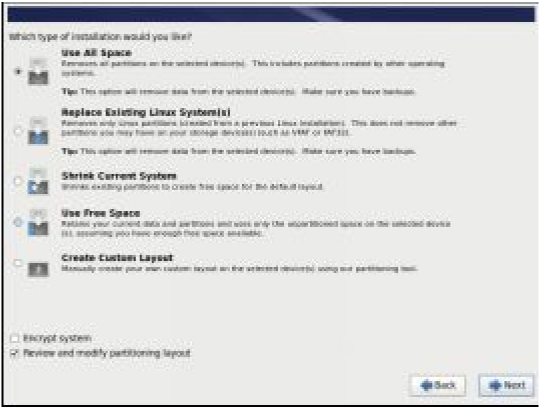


The root account is used for administering the system. Enter a password for the root user.

Root Password:

Confirm:

. Select use all, tick **Review and modify partitioning layout** before pressing next.



Which type of installation would you like?

● **Use All Space**
Removes all partitions on the selected device(s). This includes partitions created by other operating systems.

Tip: This option will remove data from the selected device(s). Make sure you have backups.

○ **Replace Existing Linux System(s)**
Removes only Linux partitions (created from a previous Linux installation). This does not remove other partitions you may have on your storage device(s) (such as VFAT or FAT32).

Tip: This option will remove data from the selected device(s). Make sure you have backups.

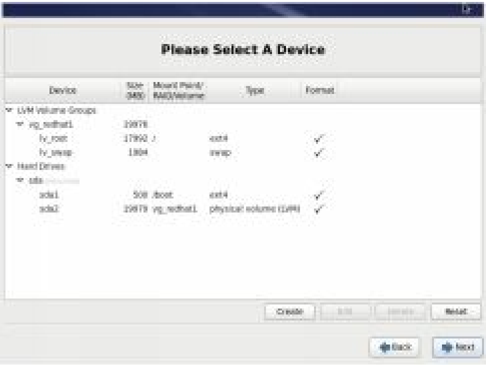
○ **Shrink Current System**
Shrinks existing partitions to create free space for the default layout.

○ **Use Free Space**
Retains your current data and partitions and uses only the unpartitioned space on the selected device (s), assuming you have enough free space available.

○ **Create Custom Layout**
Manually create your own custom layout on the selected device(s) using our partitioning tool.

□ Encrypt system
☑ Review and modify partitioning layout

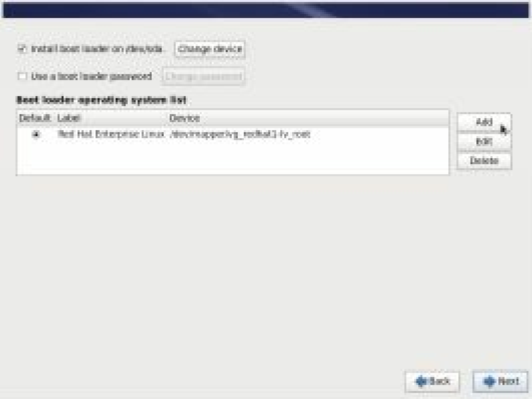
. Here you can edit the layout



Please Select A Device

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
▾ LVM Volume Groups				
▾ vg_redhat1	19976			
lv_root	17992	/	ext4	✓
lv_swap	1984		swap	✓
▾ Hard Drives				
▾ sda				
sda1	500	/boot	ext4	✓
sda2	19979	vg_redhat1	physical volume (LVM)	✓

. Confirm to write to disk in the next screen it will ask you to confirm the location boot loader click next.



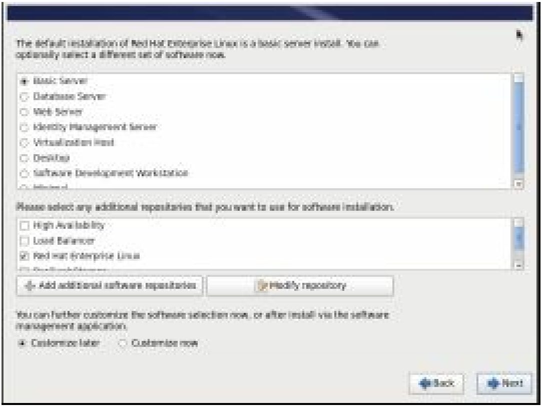
☑ Install boot loader on /dev/sda. Change device

☐ Use a boot loader password Change password

Boot loader operating system list

Default	Label	Device
●	Red Hat Enterprise Linux	/dev/mapper/vg_redhat1-lv_root

. Next is the Software package selection menu Press **next** with default selected if you want command line interface after installation. If you want graphical desktop click **customize now**.



The default installation of Red Hat Enterprise Linux is a basic server install. You can optionally select a different set of software now.

- ● Basic Server
- ○ Database Server
- ○ Web Server
- ○ Identity Management Server
- ○ Virtualization Host
- ○ Desktop
- ○ Software Development Workstation

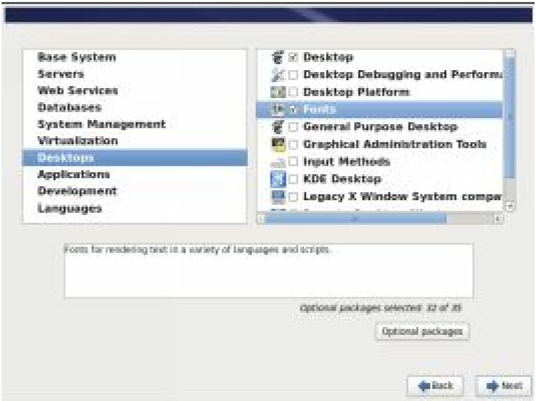
Please select any additional repositaries that you want to use for software installation.

- □ High Availability
- □ Load Balancer
- ☒ Red Hat Enterprise Linux

You can further customize the software selection now, or after install via the software management application.

● Customize later ○ Customize now

. On the next screen in left pan select **Desktops** and on right pan select **Desktop** and **Fonts.**



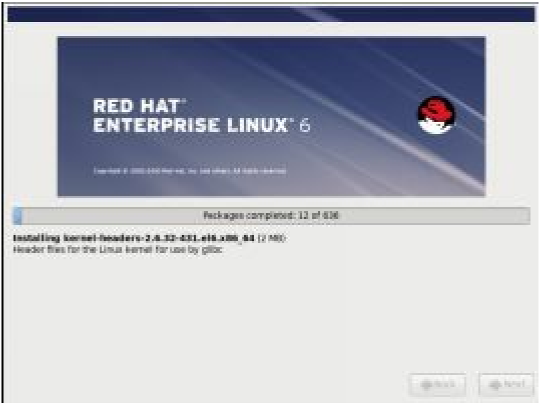
Base System
Servers
Web Services
Databases
System Management
Virtualization
Desktops
Applications
Development
Languages

☑ Desktop
□ Desktop Debugging and Perform
□ Desktop Platform
☑ Fonts
□ General Purpose Desktop
□ Graphical Administration Tools
□ Input Methods
□ KDE Desktop
□ Legacy X Window System compa

Fonts for rendering text in a variety of languages and scripts.

Optional packages selected: 32 of 35

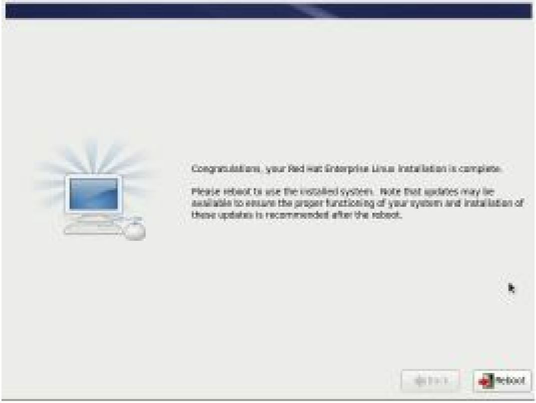
It will start install the packages.



Packages completed: 12 of 636

Installing kernel-headers-2.6.32-431.el6.x86_64 (2 MB)
Header files for the Linux kernel for use by glibc

. Once installation is finished press **Reboot**.



Congratulations, your Red Hat Enterprise Linux installation is complete.

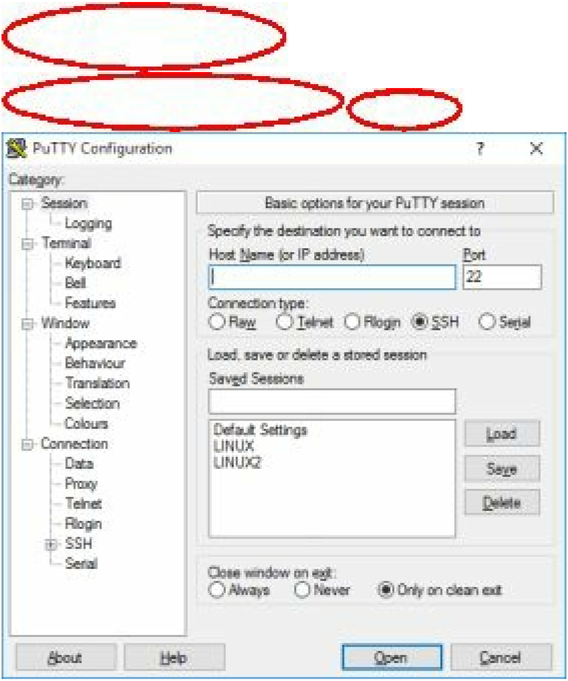
Please reboot to use the installed system. Note that updates may be available to ensure the proper functioning of your system and installation of these updates is recommended after the reboot.

. After rebooting you will get login prompt

Connecting MS windows PC to Linux machine

1. Download putty from http://www.chiark.greenend.org.uk/~
2. Install putty on windows PC

3. After installation start putty



PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - Telnet
  - Rlogin
  - SSH
  - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
LINUX
LINUX2

Close window on exit: ○ Always ○ Never ● Only on clean exit

4. Wite the IPaddress of the linux machine and name of session and

save

5. Double click the session name to connect to the Linux Machine.

Chapter 3

Network

Network allows to inter connect different machine. You require network card on computer to connect. Every network card has physical address called as media access control address (MAC address). MAC address works on layer 2 of OSI model. Manufacturer of network interface card assigns MAC addresses. To access the network card we assign IP address to network card, which works on layer 3 of OSI model. Hosts on different network can connect using layer3. As IP address are still numeric value it is difficult to remember more over there is possibility of IP address may change. To make life easy we use **hostname**.

Seven layer of OSI and TCP Mapping

OSI Model	TCP Model	Application	Addres
7:Application layer	Application Layer	HTTP / Telnet / SSH	Applications DNS, DHCP.ntp,H
6:Presentation layer		SSL / MIME	
5: Session layer		Sockets and Remote Procedure Call (RPC)	
4: Transport layer	Transport layer	Transmission Control Protocol	TCP/UDP

		(TCP)	
3: Network layer	Internet layer	Internet Protocol (IP)	IP4, IP6, ICMP
2: Data link layer	Network Access Layer	Ethernet / Frame Relay	MAC add ARP
1: Physical layer		IEEE 802.x	Ethernet

Check IP address and routing table

Show IP address

```
# ip addr show
```

Or

```
# ifconfig -a
```

Show Link status

```
# ip link show
```

Show routing table

```
# ip route
```

Or

```
# netstat -rn
```

Check and change hostname

Show hostname

```
# hostname
```

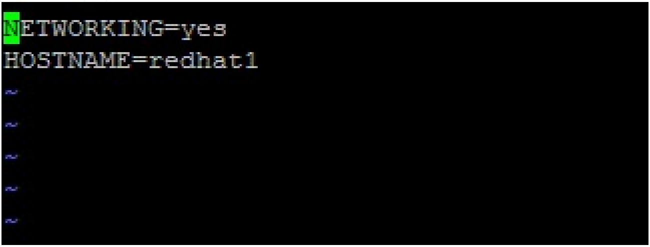
Change hostname

Whenever you want to change hostname, you have to change it at two places

/etc/sysconfig/network
/etc/hosts

First Change **/etc/sysconfig/network** file and change hostname to your new hostname in this example it is redhat1.

```
# vi /etc/sysconfig/network
```



```
NETWORKING=yes
HOSTNAME=redhat1
~
~
~
~
~
```

Next step is to change **/etc/hosts** file

```
 127.0.0.1 redhat1 localhost.localdomain
localhost
```

Setting Up the DNS Name Resolution

Whenever you write hostname instead of IP address to ping or to connect Linux host. You have multiple option to resolve hostname to IP address.

- Local file i.e. /etc/hosts
- DNS server
- NIS

/etc/hosts

Using local file **/etc/hosts** for hostname to IP address mapping provides ability to store list of hostname to their respective IP address you don’t require to look for DNS server. It is also useful if you are connecting to limited servers due scope or security reason you do not have to depend on DNS server.

Format

```
IP_address    hostname aliases
```

Example

```
127.0.0.1                          redhat1
localhost
::1                        redhat1 localhost
192.168.228.129             redhat2
```

Using Domain Name Server for name resolution

/etc/resolv.conf

To resolve hostnames to IP addresses system reads a file called **resolv.conf**. You need to put your DNS server IP addresses in this file. Generally, you need one name server, but you can include up to three if you want redundancy.

If the first one on the list is not responding, system tries to resolve against the next one on the list, and so on.

Edit **/etc/resolv.conf** to add list of name servers, like this:

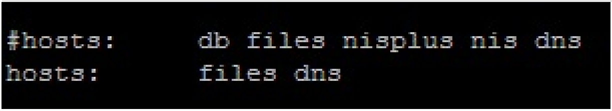
```
nameserver 8.8.8.8
nameserver 8.8.8.9
nameserver 1.2.3.6
```

Changing order for hostname resolution

/etc/nsswitch.conf

If hosts file and DNS configuration is there in **resolv.conf** in your server, Whenever you do hostname resolution the system looks for local file **(/etc/hosts)** for entry of hostname and respective IP address. If there is no entry, it looks for **/etc/resolv.conf** file for DNS configuration. If there is no DNS configuration also then it will check for NIS configuration. However, you can change this behavior by changing **/etc/nsswitch.conf**

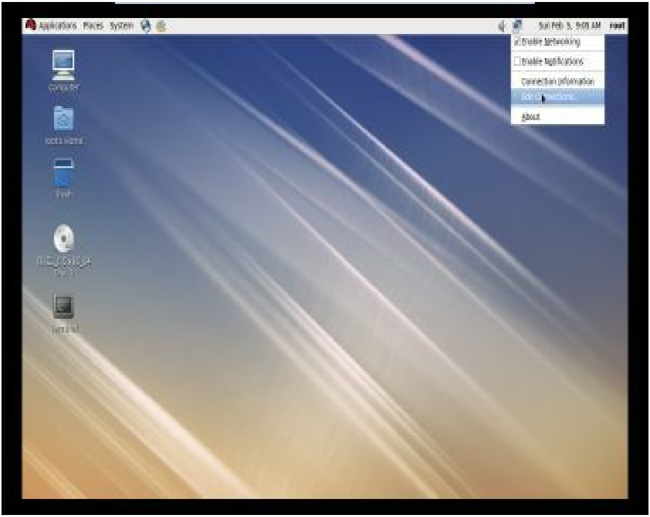
```
vi /etc/nsswitch.conf
```



```
#hosts:     db files nisplus nis dns
hosts:      files dns
```

In this example search sequence is first files means **/etc/hosts** then DNS server.

Modifying network configuration with GUI



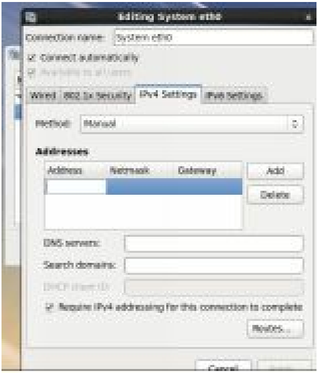
Right click network manager icon

Wired tab > edit connection >select

eth0 and edit button

Select IP4 settings

On method drop down menu change DHCP to manual



Editing System eth0

Connection name: System eth0

☑ Connect automatically

☑ Available to all users

Method: Manual

☑ Require IPv4 addressing for this connection to complete

Under address click add enter IPv4 address, netmask, gateway router and DNS server

IMPORTANT Make sure connect automatic is checked

Apply

Modifying network configuration manually

If you don’t have Graphical desktop on the host and want to change the IP address or network is not working.

Check current setting

```
# ip addr show
```

Edit **/etc/sysconfig/network-scripts/ifcfg-eth0.** You could have **ifcfg-eth0** for your first Ethernet interface **ifcfg-eth1** for Second Ethernet so on, **ifcfg-lo** for the network loopback interface.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Change **/etc/sysconfig/network-scripts/ifcfg-eth0** file depending on where you have static IP address or you are using DHCP

Static	

DEVICE=eth0
BOOTPROTO=static
IPADDR =192.168.0.132
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
ONBOOT=yes
	DEV
	BOO

Restart network services

```
# service network restart
```

Adding static route

To change static routes do the following

Check current routing table

```
# netstat -rn
```

or

```
# route -n
```

or

```
# ip route show
```

Edit /etc/sysconfig/network-scripts/route- interface file and add X.X.X.X/X via Y.Y.Y.Y dev interface Where X.X.X.X is IP address or network and Y.Y.Y.Y is gateway used by X.X.X.X

```
# vi /etc/sysconfig/network-scripts/route-eth0
```

```
10.0.0.0/8 via 192.168.1.1
```

Restart network services

```
# service network restart
```

Check the route table again

```
# route -n
```

Ping the destination address

```
# ping 10.0.0.2
```

Changing DNS server

Edit **/etc/resolv.conf**

```
search example.com          // give own FQDN
nameserver 8.8.8.8          // IPaddress of first DNS
nameserver 8.8.4.4          // IPaddress of Second DNS
```

Managing network interface

Bring down Ethernet interface eth0

```
# ifdown eth0
```

Bring up Ethernet interface eth0

```
# ifup eth0
```

Important Network Commands

Task	Command
Check connectivity between two system	ping *IP_address* Example ping 10.1.1.2
Check IP address configuration	ifconfig –a or ip addr show
Check	cat

configuration of network card	/etc/sysconfig/netw scripts/ifcfg-eth0
Check routing table	ip route show
Querying Domain Name System	dig
Local file to resolve hosts to IP address	/etc/hosts
DNS server	/etc/resolv.conf

configuration file	

Chapter 4

Managing local users and groups

As Linux is a multi-user operating system, it allows multiple users on different computers to access a single system. As a system administrator you required to perform users and group management, which include add, modify remove users and groups according to policy of the organization the server belongs to.

User management

Add User

```
# useradd username
```

Or

```
# adduser username
```

Now set the password

```
# passwd username
```

Delete user

```
# userdel username
```

Modify user

```
# usermod -c “database user” username
```

Display information about

user

`# id` show current user information

`# id username` Show users information

Change password for other user

```
# passwd username
```

Change own password

```
# passwd
```

List password expiry information

```
# chage -l username
```

Disable password expiration for user

```
# chage -I -1 -m 0 -M 99999 -E -1 username
```

Force user to change password at next login

```
# chage -d 0 user1
```

Lock user

```
# usermod -L user1
```

Unlock user

```
# usermod –U user1
```

UID

Unique User ID called as UID is every user exist on system user it fixed for root and regular users

User	UID
root	0
System user	1 – 499
Regular users	500 +

Groups

Every user we create belongs to group and all groups have group ID. List all available groups can be found in /etc/groups and entry of all users member of these groups there are two type of groups

- primary group
- secondary group

Primary group

This is the group applied to you when you login and used by default when you create new files and directories. It is normally same name as username. Users primary group ID is written /etc/passwd file for respective users in the third field.

Secondary Group

These are the groups users are member other than primary group

/etc/group

```
groupname:shadow password:GID:list of
users in group
```

Example

```
science:x:1003:class1,class2
```

Changing primary group

```
usermod –g data1  user1
```

Changing secondary group

```
usermod –G data2 user1
```

Add new group

```
groupadd groupname
```

Delete group

```
groupdel groupname
```

/etc/passwd

Stores user information

Format

```
username:x:UID:GID:Full_user_name:home_
```

Username up to 8 characters. Case-sensitive

x Passwords are stored in the ``/etc/shadow'' file.

UID User ID

GID Group ID

shell account Often set to ``/bin/bash'' to provide access to the bash shell but can other shell like c shell korn shell

Example

```
root:x:0:0:root:/root:/bin/bash
```

/etc/shadow

Stores actual password in encrypted format

Format

```
username:password:last_password_change:mi
```

Username up to 8 characters. Case-sensitive, usually all lowercase. A direct match to the username in the /etc/passwd file.

Password 13 character encrypted. A blank entry (eg. ::) indicates a password is not required to log in (usually a bad idea), and a ``*'' entry (eg. :*:) indicates the account has been disabled.

last_password_change The number of days (since January 1, 1970) since the password was last changed.

Minimum: The number of days before password may be changed (0 indicates it may be changed at any time)

Maximum: The number of days after which password must be changed

(99999 indicates user can keep his or her password unchanged for many, many years)

Warn : The number of days to warn user of an expiring password (7 for a full week)

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

Expire: The number of days since January 1, 1970 that an account has been disabled

Example

```
root:$6$YtTXd..cW9GYuWT9sNwX07B3i.:17
```

Chapter 5

NFS Network File System

NFS is file sharing file system which works on server client basis. Server's shared file systems are mounted on client. Four version of NFS are there:-

1. NFS V1
2. NFS V2
3. NFS V3
4. NFS V4

Where NFS V3 and NFS V4 are more recent version of NFS, V3 is safer and asynchronous works on UDP protocol while V4 has added advantage of working through firewall and works on TCP.

/etc/exports

Configuration file used to export file system on server to clients

To export file system without /etc/exports manually.

```
# exportfs –i /user1
```

To unexport all exported file

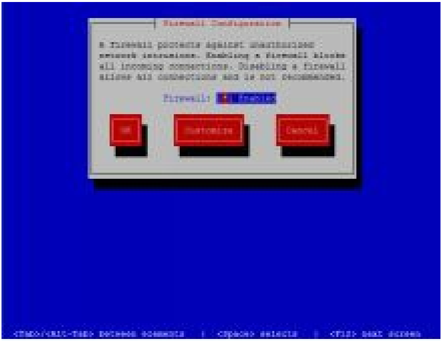
system

```
# exportfs –ua
```

Configure NFS on the server without firewall

Disable firewall

System-config-firewall-tui > unselect the firewall **enable >** ok



Firewall Configuration

A firewall protects against unauthorized network intrusions. Enabling a firewall blocks all incoming connections. Disabling a firewall allows all connections and is not recommended.

Firewall: [*] Enabled

OK
Customize
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

```
# service iptables stop
```

Install packages

```
# yum install nfs-utils
# yum install rpcbind
```

or

```
# yum groupinstall 'NFS file server'
```

Start the services

```
# service rpcbind start
# service nfs start
```

Make service start on next reboot

```
# chkconfig nfs on
# chkconfig rpcbind on
```

Edit /etc/exports file to add filesystem you want to share to clients format of that is :-

```
mountpoint      [host][permissions/options]
```

where

mountpoint is file systems you want export

host is optional the client you want to give access the file systems

permissions is optional it can be **ro** read only ,**rw** read write **insecure**, **sync** changes written before command finished.

Export file system

```
# exportfs –a
```

See the file system exported

```
# showmount –e
```

On client

```
# showmount –e server IP address / hostname
# mount –t nfs 192.168.0.1:/userfs /newmnt
```

Mounting DVD automatically

Make directory for mounting

```
# mkdir /cdrom
```

edit the /etc/fstab file

```
# vi /etc/fstab
```

add following line

```
/dev/cdrom      /cdrom          iso9660
ro              0 0
```

reboot the server

check mount

```
# mount
```

Chapter 6

Graphics User Interface

When you install Linux distribution, you have option to install GUI desktop environment, which makes administration easy.

There are many desktop environments are available from which prominent are:-

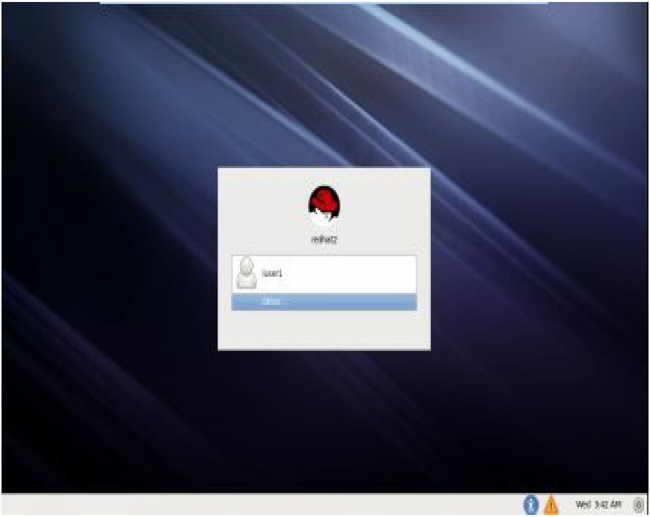
- GNOME
- KDE
- XFCE
- LXDE

GNOME is the default desktop

environment for RedHat.

Graphical Login

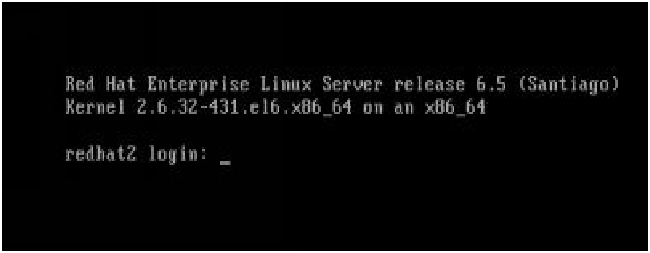
When you start the machine, you will get login window



You select **other** to log in as root from the graphical login screen, type root at the login prompt, press **[Enter]**, type the root password that you selected during installation at the password prompt, and press **[Enter]**. To log in as a normal user, select username at the login prompt, press **[Enter]**, type your password that you selected when creating the user at the password prompt, and press **[Enter]**.

Virtual Console Login

When install Linux with Graphical desktop, usually you get six virtual consoles provide a text terminal with a login prompt to Linux shell. The graphical X Window System starts in the seventh virtual console. User switches between them with the key combination Alt plus a function key – for example Alt+F1 to access first virtual console. During installation, if you haven’t selected graphical desktop you will see a login prompt similar to the following after booting your system



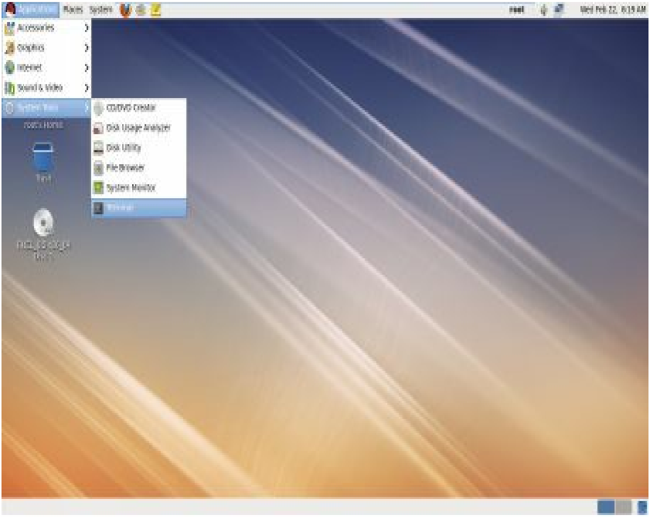
```
Red Hat Enterprise Linux Server release 6.5 (Santiago)
Kernel 2.6.32-431.el6.x86_64 on an x86_64

redhat2 login: _
```

To log in from the console, type username at the login prompt, press Enter, then type the password and press Enter.

GNOME terminal

Gnome terminal is terminal emulator for gnome desktop environment. Terminal allows to you give command to your redhat machine. By default you gets the **>** prompt if you login as normal user and **#** prompt if you login as root . To change to # prompt from > you use **su** command and password of root. To open Gnome Terminal Applications > System Tools > Terminal.



Commands

Ctrl +a	Moves the cursor to the beginning of the command prompt
Ctrl + e	Moves the cursor to the

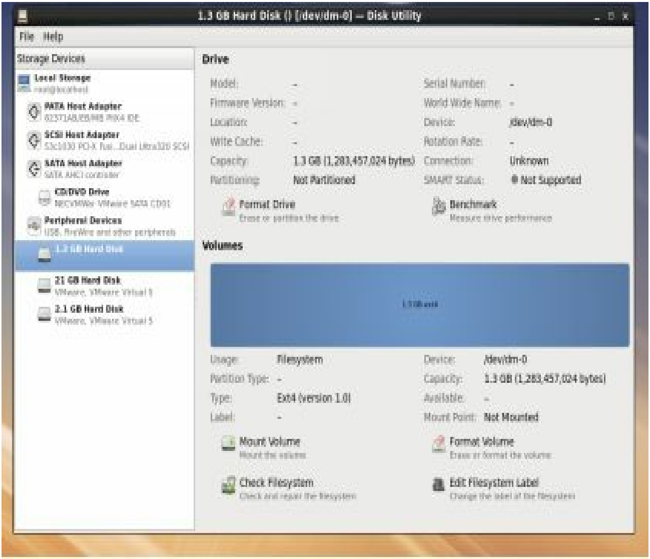
	end of the command prompt
Ctrl + u	Clear the current line
Middle mouse button click	Paste the highlighted text
Tab	Completes the command
Up / Down Keys	Show history of commands
Ctrl +c	Terminate the current process
Ctrl + z	Suspends the foreground process

Disk Utility

With graphical disk utility you can

- Create / Delete / Edit partition
- Mount / Unmount file system
- Format volume to required File System Type
- Check File System
- Edit File system label
- Format drive
- Check benchmarks

From left pan select the required device then you can do operation on the device.



Drive

Model: -
Serial Number: -
Firmware Version: -
World Wide Name: -
Location: -
Device: /dev/dm-0
Write Cache: -
Rotation Rate: -
Capacity: 1.3 GB (1,283,457,024 bytes)
Connection: Unknown
Partitioning: Not Partitioned
SMART Status: ● Not Supported

Volumes

Usage: Filesystem
Device: /dev/dm-0
Partition Type: -
Capacity: 1.3 GB (1,283,457,024 bytes)
Type: Ext4 (version 1.0)
Available: -
Label: -
Mount Point: Not Mounted

Chapter 7

Process and threads

Every task done by Linux OS has process associated with it. Process has priority based on the context switches on them.

Each process provide resources needed to execute the program

Each process starts with single thread known as primary thread. Process can have multiple threads.

Process runs in foreground and background

Commands

Command	Description
bg	Sends job to Background
fg	Bring job to foreground
jobs	Show current jobs
kill	Stops the process
ps	Show the process information
&	if command ends with the & the shell execute the command in background and shell

	will not wait for finish Example gcalctool &

Bring command to foreground

```
# fg
ctrl + c
```

Check the running jobs

```
# jobs
```

List the current running process

```
# ps –ef |grep gcalctool
```

or

```
# ps aux
```

Kill the process forcefully

First check the process ID with `ps –ef` command then

```
# kill -9 <process –id >
```

Monitoring the process with ps command

ps command show the percentage of CPU & memory utilization of the process it is very useful if your machine is under performing. **ps** command gives you indication which process is hogging memory/CPU.

Process scheduling

Scheduler is part of kernel, which select process to run next. The purpose is to run the processes according to priorities. To set the priority of running process nice and renice command is used which decide how longer or smaller CPU time is given to process.

nice set the priority or niceness of new process.

renice adjust nice value of running process

niceness of -20 is higest prority and 19 is lowest priority. The default prirotity is 0

Example

```
# nice –n 19 cp –r /as /map
```

Commands show priorities of running processes

```
# ps –al
```

or

```
# top
```

To change the priority

```
# renice –n 10 <pid>
```

Note: You need root privilege to change to higher priority.

Chapter 8

Automating tasks

Redhat has utilities to automate the task which system administrator do regularly or at specified time. Following are the main utilities

- cron
- at
- batch

Cron

cron is daemon that can be used to schedule the execuction of recurring tasks according to time, day of month, day of week .

Configuration file

/etc/crontab

Command

Command	Description
crontab –l	List crontab entries
crontab –e	Edit crontab
crontab –r	Remove crontab

Format

```
minutes hours Day_of_month
Month         Day_of_week     Command
```

Where

Minutes	(from 0 to 59)
hours	(from 0 to 23)
day of month	(from 1 to 31)
month	(from 1 to 12)
day of week	(from 0 to 6) (0=Sunday)

To schedule a recurring task

Edit crontab by giving command

```
crontab -e
```

Add entries at bottom of file press **i**

Suppose you want to run backup script every night at 11:30

```
30    23 * * *   /myscripts/backup.sh
```

Press [escape] and press **:** write **x** after that press [enter] to save the entry

at and batch

crontab is used for recurring task but for one time tasks at specified time **at** and **batch** commands are used.

To run at command rpm must be installed and **atd** service must be running

Check Installation

```
# rpm –q at
```

Install at package

```
# yum install at
```

Start service

```
# service start atd
```

Start command

```
# at 4:00
at > ls
ctrl + d
```

Batch command executes one time task when system average load decreases bellow 0.8

```
# at
at > ls
ctrl + d
```

Display list of pending jobs

```
atq
```

Chapter 9

Log management

Log files are very useful in troubleshooting and auditing system for authorized system access. In Redhat 6 some logs are controlled by rsyslogd daemon. It is enhanced replacement of **sysklogd**. It offers high-performance, great security features, modular design and support for transportation via the TCP or UDP protocols.

rsyslogd reads the file **/etc/rsyslog.conf. rsyslogd** can be configured vai **rsyslog.conf** file. List of log files maintained by **rsyslogd** can be found in the rsyslog.conf configuration file. Log files are usually located in the /var/log/ directory.

install

```
# yum install rsyslog
```

Configuration file

/etc/rsyslog.conf

Sample rsyslog.conf

```
[root@redhat1 etc]# cat rsyslog.conf
# rsyslog v5 configuration file

# For more information see /usr/share/doc/rsyslog-
```

```
*/rsyslog_conf.html
# If you experience problems, see
http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

$ModLoad imuxsock # provides support for local
system logging (e.g. via logger command)
$ModLoad imklog   # provides kernel logging
support (previously done by rklogd)
#$ModLoad immark  # provides --MARK--
message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
```

```
#$InputTCPServerRun 514


#### GLOBAL DIRECTIVES ####

# Use default timestamp format
$ActionFileDefaultTemplate
RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This
feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf


#### RULES ####
```

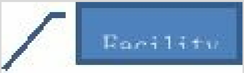
```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*
/dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none
/var/log/messages

# The authpriv file has restricted access.
authpriv.*
/var/log/secure

# Log all the mail messages in one place.
```

```
mail.*
-/var/log/maillog
```



```
# Log cron stuff
```

```
cron.*
/var/log/cron

# Everybody gets emergency messages
*.emerg                                         *

# Save news errors of level crit and higher in a
```

```
special file.
uucp,news.crit
/var/log/spooler

# Save boot messages also to boot.log
local7.*
/var/log/boot.log
```

Log filtering

There is too much logging happens in the system if it is not filtered it become almost impossible to use logs. To filter the logs we use **/etc/rsyslog.conf** file. It has two parameter facility and priority separated with dot(.). Facility is name of process for which you want to log and priority specify level of log like debug, info, notice, warning, err, crit , alert, emerg you want to keep.

Example

```
# The authpriv file has restricted access.
```

```
authpriv.*
/var/log/secure

# Log all the mail messages in one place.
mail.*                                                -
/var/log/maillog
```

In the example where **authpriv** and **mail** is facility and ***** is priority mean all logs.

Rotating logs

Logs needs rotation to avoid filling of file systems and make log more manageable.

Once log file is rotated, it will be renamed with new file name. After certain time of rotation older log files will get deleted to save space.

logrotate package manages automatically rotating of log files according to configuration in /etc/logrotate.conf

logwatch

logwatch is program to analyze and reporting short digest via mail. Can be configured vai **/usr/share/logwatch/default.conf/logwa** configuration file.

Install

```
# yum install –y logwatch
```

Configure

Setting configuration file **/usr/share/logwatch/default.conf/logwa**

The email address to which daily

digest(report) are sent

mailto =root

Example

```
# Default person to mail reports to.  Can be a
local account or a
# complete email address.  Variable Print
should be set to No to
# enable mail feature.
MailTo = root
```

Chapter 10

Software management

Redhat network

Red Hat Network is a centrally managed service provides facility to deploy software and software updates to Red Hat Enterprise Linux systems. To receive updates for Redhat server you have get subscription of Redhat network.

To register your system with RHN :-

- Go to Redhat customer portal and create user

Add your subscriptions

Connect server to internet

Give command **subscription-manager register**

```
# subscription-manager register
Username: abc74
Password:
The system has been registered with ID:
bb304a30-c30e-4bb7-9d41-xxxxxx
```

Determine the pool ID you want to Add by listing all pools

```
subscription-manager list --available
subscription-manager register
Username: abc74
```

```
Password:
The system has been registered with ID: bb304a30-c30e-4bb7-9d41-xxxxxx
[root@redhat1]# subscription-manager list --available
+-------------------------------------------+
   Available Subscriptions
+-------------------------------------------+
Subscription Name: 30 Day Self-Supported Red Hat Enterprise Linux Developer Workstation Evaluation
```

Attach your system to desired subscription

subscription-manager attach --pool=pool_id

Now list how many subscriptions are consumed

subscription-manager list –consumed

Repository

Repository is collection of software for linux, ether present locally or remotely. The repository can be used to install additional software or to update the current software. When you subscribe to RHN a repository file is created **/etc/yum.repos.d/** directory.

Display all enabled repositories

```
# yum repolist
```

Display all repositories

enabled and disabled

```
# yum repolist all
```

yum

Yellow dog updater modifier is command line tool for package management. yum uses repository to fetch the correct version of a particular package compatible for your system. Yum allows automatic update of packages and dependency management. It allows automatically download the packages and install them form repositories either RHN or local repository defined such as CDROM or directory. You can also use third party reposiroties to install extra packages like open office, VLC etc.

Commands

Package

Install package

Syntax

```
# yum install –y package_name
```

Example

```
# yum install –y firefox
```

Remove package

Syntax

```
# yum remove package_name
```

Example

```
# yum remove firefox
```

Check available updates

```
#cyum check-update
```

Update system using yum

```
# yum update
```

Check the file provided by which package

```
# yum provides file-name
```

Get help

```
# yum help
```

list the installed and available software

```
# yum list
```

search the package name

with keyword

```
# yum search keyword
```

Display information about the package

Syntax

```
# yum info package_name
```

Example

```
# yum info zip
```

Update all software provided by the repository

```
# yum update
```

Clean the yum cache

```
# yum clean all
```

Interactive shell

```
# yum shell
```

List yum history

```
# yum history list
```

Package group

Package group is group of software which has same motive to install. It makes administrator’s life easy by installing and downloading dependent software automattically. For example, you want to install KDE Desktop environment you give command **yum groupinstall 'Backup Client'**

List all package group available

```
# yum grouplist
```

Install group package

Syntax

yum groupinstall *package_name*

Example

```
# yum groupinstall 'Backup Client'
```

Remove group package

Syntax

yum groupremove *package_name*

Example

```
# yum groupremove 'Backup Client'
```

Information about group package

Syntax

yum groupinfo *package_name*

Example

```
# yum groupinfo 'Backup Client'
```

Installing packages with RPM command

RPM

RPM stands for Red Hat Package Manager. RPM packages have .rpm extension. **rpm** command is used to manage software which include list, install, update and remove . RPM is usually used to install packages which has been downloaded locally

Commands

Install

Syntax

rpm -ihv package_name

Example

```
[root@redhat1 Packages]# rpm -ihv zip-3.0-
1.el6.x86_64.rpm
Preparing...
####################################
[100%]
   1:zip
####################################
[100%]
```

Update

Syntax

rpm –Uhv package_name

Example

```
# rpm –Uhv zip-3.0-1.el6.x86_64.rpm
```

Remove

Syntax

```
rpm –ev package_name
```

Example

```
# rpm -ev zip
```

Query all installed packages

Syntax

```
rpm -qa
```

Display detailed information about package

Syntax

rpm –qi package_name

Example

```
rpm -qi zip
Name        : zip                 Relocations: (not
relocatable)
Version     : 3.0                       Vendor: Red
Hat, Inc.
Release     : 1.el6                    Build Date:
Mon 24 May 2010 07:53:44 PM IST
Install Date: Sun 12 Feb 2017 10:05:18 AM
IST     Build Host: x86-
005.build.bos.redhat.com
Group       : Applications/Archiving      Source
RPM: zip-3.0-1.el6.src.rpm
Size        : 823612                     License:
BSD
Signature   : RSA/8, Tue 17 Aug 2010 02:05:20
```

```
AM IST, Key ID 199e2f91fd431d51
Packager    : Red Hat, Inc.
<http://bugzilla.redhat.com/bugzilla>
URL         : http://www.info-zip.org/Zip.html
Summary     : A file compression and packaging
utility compatible with PKZIP
Description :
The zip program is a compression and file
packaging utility.  Zip is
analogous to a combination of the UNIX tar
and compress commands and
is compatible with PKZIP (a compression and
file packaging utility for
MS-DOS systems).

Install the zip package if you need to compress
files using the zip
```

program.

Find the file belongs to which package

Syntax

rpm –qf path_to_the_file

Example

```
[root@redhat1 Packages]# rpm -qf /etc/hosts
setup-2.8.14-20.el6_4.1.noarch
```

Find out all dependences

Syntax

rpm -qpR *package_name*

Example

```
[root@redhat1 Packages]# rpm -qpR zip-3.0-1.el6.x86_64.rpm
libc.so.6()(64bit)
libc.so.6(GLIBC_2.2.5)(64bit)
libc.so.6(GLIBC_2.3)(64bit)
libc.so.6(GLIBC_2.3.4)(64bit)
libc.so.6(GLIBC_2.4)(64bit)
```

Repository

To install additional package or update existing package you require repository. It is warehouse all Linux software. Yum repository can hold **RPM** packages located locally like CDROM , directory on local disk or remotely like FTP, HTTP or HTTPS. The configuration files for name, location, status etc of repository is there in **/etc/yum.repos.d/** directory.

The configuration file present in the **/etc/yum.repos.d/** directory have following fields

Repository ID - Single word unique repository ID

Name - Name of the repository (example: name=CD_media)

Baseurl - URL to the repodata directory. You can use ftp://link, http://link, https://link if repository is located remotely and file://path if repository is located locally (example file:///mnt/ for mnt directory locally)

Enabled - Enable/Disable repository (example: enabled=1 to enable or enable=0 to disable)

Gpgcheck - Enable/disable GPG signature checking (example: gpgcheck=1)

Gpgkey - location of GPG key

Defining repository

1. Create file /etc/yum.repos.d/<*name*>.repo
2. Add following contents

```
[Repository_ID]
name=name_of_repository
baseurl=http://location
enabled=1
gpgcheck=0
```

Using Red Hat DVD or local directory as repository

Mount the RHEL 6 installation ISO to a directory like /mnt, e.g.:

```
# mount -o loop RHEL6.1.iso /cdrom
```

If you use DVD media, you can mount like below.

```
# mount -o ro /dev/cdrom1  /cdrom
```

Where /dev/cdroml is DVDROM device you may have different one.

Create file name cdrom.repo in

/etc/yum.repos.d/ that should look like the following where /cdrom is directory where cdrom is mounted

```
[installmedia]
name=Red Hat Enterprise Linux 6.5
baseurl=file:///cdrom/
gpgcheck=0
enabled=1
```

Clear the related caches by **yum clean all** and **subscription-manager clean**

```
# yum clean all
# subscription-manager clean
```

Now check the repository

```
# yum repolist all
```

Chapter 11

Utilities

Tar

Use to create one archive file of multiple files used for backup on tape or other media. You also create compress file with adding option while creating achieve file.

Create tar

Syntax

```
tar cvf name_of_archive_file files_or_directory_to_archive
```

Where

c create

v verbose

f file name types of achieve file

Example

```
[root@redhat1 share]# tar cvf abc.tar *
applications/
applications/preferred-mail-reader.desktop
applications/preferred-web-browser.desktop
gvfs-metadata/
[root@redhat1 share]# ls -la
total 96
drwxr-xr-x. 4 root root  4096 Feb 12 10:58 .
drwxr-xr-x. 3 root root  4096 Feb  4 12:46 ..
-rw-r--r--. 1 root root 81920 Feb 12 10:58 abc.tar
```

Create compressed tar file

Create gzip format tar file

```
# tar cvfz abc.tar.gz name_of_files
```

Create bzip format

```
# tar cvfj abc.tar.bz2 name_of_files
```

untar

```
# tar xvf abc.tar
```

Where

x	extract
v	verbose
f	file name types of achieve file

Uncompressing

Uncompressing gzip format

Syntax

```
tar xvfz filename
```

Example

```
# tar xvfz abc.tar.gz
```

Create bzip format

Syntax

```
tar xvfj filename
```

Example

```
# tar xvfj abc.tar.bz2
```

List the archived tar file

Syntax

```
tar tvf filename
```

Example

```
# tar tvf abc.tar
```

List gzip compressed tar file

Syntax

tar tzvf filename

Example

```
# tar tzvf abc.tar.gz
```

List bgzip compressed tar file

Syntax

tar tjvf filename

Example

```
# tar tjvf abc.tar.bz2
```

cp

Command to copy files

Syntax

cp <options> source destination

Example

```
cp /home/abc.txt /home1/
```

Copy all files in the directory recursively

```
cp –R  /home/* /home1/
```

Prompt before any overwrite

```
# cp –i /home /home1
```

Copy all new files to the

destination

```
# cp –u * /tmp
```

Forcefully copy files

```
# cp –f /tmp/abc.txt /backup/.
```

Copy without prompting to overwrite

```
# cp -n * t
```

scp

scp command is used to copy files form one host to other host in secured manner.

Copy files from local machine to remote machine

Syntax

```
scp filename remote_user@remote.host:/some/remote_diec
```

copy xyz file from remote host to local host

Syntax

```
scp
```

remote_user@remote.host:/some/remote_diec

.

CPIO

Copy files from and to achieve. Used for creating and extracting achieve and also for coping files from one place to another.

Creating achieve form directory abc to /directory backup

```
# cd abc
# ls |cpio –ov > /backup/abc.cpio
```

Extracting

```
# mkdir newbackup
# cd newbackup
# cpio idv < /backup/abc.cpio
```

Creating archive of list of specific files.

Example :- archieve all log files

```
# find . –iname *.log –print|cpio –ov >
/backup/selog.cpio
```

Using cpio to create tar file

```
# ls|cpio –ovH tar –F abc.tar
```

To extract tar file using cpio

```
# cpio –idv –F abc.tar
```

Dump and Restore

dump

Dump utility backup whole file system or files that has changed since last dump ideally dump should be taken on the quiescent file system, so that files are not changing while backup.

Syntax

```
dump <options> target_device filessystem_tobe backed_up
```

Example :

To take backup of whole root filesystem to device st0

```
# dump –0uf /dev/st0 /
```

Where

0 is dump level. There are ten dump levels from 0 to 9

0 complete

1 increment from last backup

2 increment from last 1 backup

3-9 like that

u updates /etc/dumpdates file with dump information

f for device name

restore

restore command is used to restore the backup taken with dump command

syntax

restore <options> backupdevice

Example:

To restore backup stored on /dev/st0 device

```
# restore –if /dev/st0
```

where option

i invokes interactive mode that allows you to choose which file and directory to restore

f is for device name

Restore specific file

To restore specific file from backup in this example to restore /**etc/hosts** file

```
# restore –xf /dev/st0 /etc/hosts
```

ls

Lists the Names of Files

Syntax

```
ls -<options>
```

Example

`# ls -al` To list directories and files

cat

Displays a Text File

Syntax

cat filename

Example

```
# cat abc.conf
```

rm

Deletes a file, files or directory

Syntax

rm filename

Example

```
rm abc.conf
```

To delete abc directory recursively

```
rm -r abc
```

More

When you want to view a file that is longer than one screen, you can more utility. More is used for paging through text one screen full at a time.

Syntax

```
more filename
```

Example

```
# more /etc/hosts
```

less

Less is a program similar to more, but it allows backward movement in the file as well as forward movement.

Syntax

```
less filename
```

Example

```
# less /etc/hosts
```

mv

mv command is used to move file form one location to other location. It is also use rename the file without moving it.

Moving file

Syntax

```
mv filename destination_directory
```

Example

```
mv a.txt /tmp/.
```

It will move a.txt file from current directory to /tmp directory

To rename

Syntax

```
mv filename newfilename
```

Example

```
mv a.txt b.txt
```

grep

Searches for a String from one or more files. Display each line which has string.

Syntax

grep string file

Example

```
# grep '127.0.0.1' /etc/hosts
```

# head

Print the first 10 lines of file to standard output. You can also specify how many line it will show.

Syntax

```
head option file
```

Example

`# head -20 /etc/mime.types` it will show first 20 lines of mime.types file

tail

Print the last 10 lines of file to standard output. You can also specify how many line it will show.

Syntax

tail option file

Example

```
# tail -20 /var/log/logfile
```

it will show last 20 lines

Use tail to monitor file continuously

```
# tail -f /var/log/logfile
```

It will show end of growing file. **Ctrl +c** to interrupt

Diff

Compares Two Files.

Syntax

diff First_file Second_file

Example

```
# diff abc.txt bbc.txt
```

File

Determine file type

Syntax

file file_name

Example

```
# file bbc.txt
```

Echo

Display text

Syntax

echo text

Example

```
# echo hello
```

Date

Print or change the system data and time.

Syntax

date

Example

`# date` To check date

`#` `date -s "24 feb 2017 19:00"` To set date

Chapter 12

Piping and Redirection

Sending output to file (>)

Normally, we will get our output on the screen, but if we wish to save it into a file the greater than operator (>) is used to send the standard out to file.

Example

```
# ls > abc.txt
```

Sending input from file (<)

If we use the less than operator (<) then we can read data from file and feed it into the program via it's STDIN stream.

Example

```
# wc -l < abc.txt
```

Piping (|)

For sending data from one program to another we use pipe (|)

```
# ls | head -10
```

Chapter 13

Compression utilities

There are mainly three utilities to zip the files

Compression	Extension	Uncompress
bzip2	bz2	bunzip2
Gzip	gz	gunzip
Zip	zip	unzip

Compress

Bzip2 format

Syntax

bzip2 file_to_backups filename

Example

```
# bzip2 * abc
```

gzip format

Syntax

gzip file_to_backups filename

Example

```
# gzip * abc
```

zip format

zip file_to_backups filename

Example

```
# zip * abc
```

Uncompress

Bzip2 format

Syntax

bzip2 filename

Example

```
# bunzip2 abc.bz2
```

gzip format

Syntax

gunzip filename

Example

```
# gunzip abc.gz
```

zip format

Syntax

```
unzip filename
```

Example

```
# unzip abc.zip
```

Chapter 14

Managing services and daemons

Daemons

Daemons are processes, which run in the background and not interactively. Daemons perform some predefined actions at predefined time. Generally daemons start at bootup and remain till shutdown. Mostly daemons name ends with **d**.

Services

Services are init scripts (initialization scripts) resides in **/etc/rc.d/init.d** directory. These scripts are to manage daemons. Service scripts can be called with start, stop, restart, status and reload argument to manage daemons.

Service can be start at boot time using **chkconfig service_name on** command

Run level

Run level is state or mode of OS in which it will run. Each run level has certain number of services stopped or started providing control over behavior of machine. There are seven Runlevels

0 halt the machine

1 single user mode

2 not used, can be used by user

3 multiuser with command line no GUI

4 not used, can be used by user

5 multiuser with GUI

6	reboot

Commands

Check current runlevel

```
# runlevel
```

Change default run level

Edit **/etc/inittab** file in this example whe change to command line runlevel 3

```
Id:3:default:
```

Managing services startup

To list all services and there status at each runlevel

```
# chkconfig --list
```

To list current setting of specific service

Syntax

```
# chkconfig --list service_name
```

Example

```
# chkconfig --list vsftpd
```

Enabling service in runlevel 2, 3, 4 ,5

Syntax

```
# chkconfig  Service_name on
```

Example

```
# chkconfig httpd on
```

To enable at specific run level

```
# chkconfig service_name --level 35
```

To disable service for 2, 3, 4, 5 runlevel

Syntax

```
# chkconfig service_name off
```

Example

```
chkconfig httpd off
```

To disable for specific run level

Syntax

```
# chkconfig service_name off --level 3
```

Example

```
# chkconfig service_name off --level levelno
```

Managing the services status

Determine status of service whether it is running or not

Syntax

```
# service service_name status
```

Example

```
# service vsftpd status
```

Display status of all services

```
# service --status-all
```

Starting service

Syntax

```
# service  service_name start
```

Example

```
# service httpd start
```

Stopping service

Syntax

```
# service  service_name stop
```

Example

```
# service httpd stop
```

Restarting service

Syntax

```
# service  service_name restart
```

Example

```
# service httpd restart
```

Install new service

Procedure to install new service

1. Install new service package

```
# yum install service_name
```

2. Configure the service to start automatically at startup

```
# chkconfig service_name on
```

3. Start the service

```
# service service_name start
```

Example

```
# yum install vsftpd
# chkconfig vsftpd on
# service vsftpd start
```

Chapter 15

SSH

SSH provides a secure channel over unsecure network in client server architecture. SSH is a replacement of telnet, which is insecure protocol. It allows secure channel to login and execute command securely because all communication between client and server is encrypted.

ssh –x user@hostname

whenever ssh connection is made to system first time the public key of remote system is stored locally so it is identity can be verified next time.

Ctrl + d or exit command will terminate **ssh** session.

If you are connecting form MS windows client to Linux server you require third party software like **putty**.

ssh key

ssh keys helps in identifying yourself to an server using public key cryptography and challenge response authentication. ssh keys are generated in pair one public and private key. The public is for sharing and private key is for you. It must be kept safely.

Server having public key can send challenge which can only be answered by server holding private key. This allows password less login.

Password less login to server from one server in this example redhat1 to host redhat2.

Create keys on **redhat1** host

```
[root@redhat1 ~]# ssh-keygen
```

Copy public key from **redhat1** to second server **redhat2** host

```
[root@redhat1 ~]# scp ~/.ssh/id_rsa.pub
```

```
root@redhat2:/root/id_rsa.server1.pub
```

On second server **redhat2** create directory .ssh in the home directory in our case the user is root its home directory is /root and change permissions.

```
[root@redhat2 ~]# mkdir .ssh
[root@redhat2 ~]# chmod 700 .ssh
```

Append the public key file to **authorized_keys** file and change permissions.

```
[root@redhat2 ~]# cat id_rsa.server1.pub >>
.ssh/authorized_keys
```

```
[root@redhat2 ~]# chmod 644
.ssh/authorized_keys
```

Now try login form server one i.e **redhat1** to second server i.e. **redhat2** it will not ask for password.

```
[root@redhat1 ~]# ssh root@redhat2
```

Chapter 16

VNC

VNC Virtual Network Computing is graphical desktop sharing system. Used to get GUI desktop of Linux server remotely. In this VNC client is installed on local machine, which is used to connect to VNC server installed on remote server.

To configure VNC on server whose desktop you want to share

install

```
# yum install tigervnc-server
```

Add user

Edit **/etc/sysconfig/vncserver** first change word **root** to any other user you want to configure. Secondly remove -localhost this option prevent VNC to connect remotely through ssh .

```
# VNCSERVERS="2:luser1"
# VNCSERVERARGS[2]="-geometry
800x600 -nolisten tcp "
```

Set VNC password

```
# su user_name
# vncpasswd
```

Start and enable the VNC service

```
# service vncserver start
# chkconfig vncserver on
```

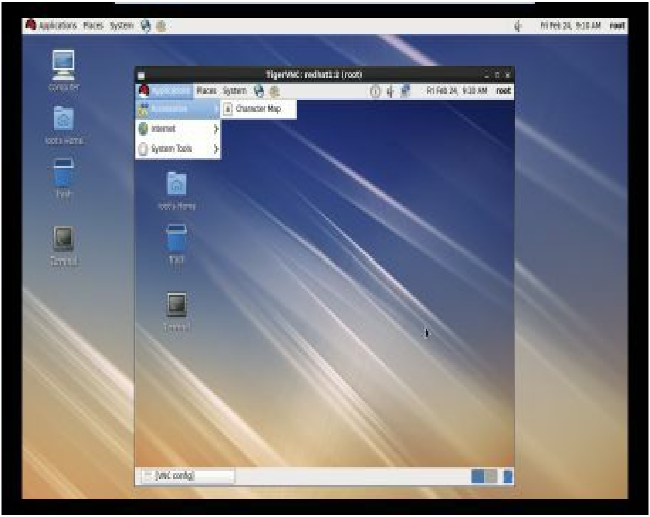
Install vncviewer on the remote machine

```
#yum install tigervnc
```

Connect on remote machine

Go to Desktop of linux box open terminal

```
#vncviewer via username@servername
localhost:2
```


Applications
Places
System
Fri Feb 24, 9:10 AM
root
Computer
root's Home
Trash
Terminal
TigerVNC: redhat1:1 (root)
Applications
Places
System
Fri Feb 24, 9:10 AM
root
Accessories
Character Map
Internet
System Tools
root's Home
Trash
Terminal
[VNC config]

Chapter 17

FTP

FTP is file transfer protocol. It used to transfer files between the computers on the network. It’s based on client server model. There can be three type of client

1. GUI
2. Web browser
3. Command line

In Redhat and derivatives distros **vsftp** (very secure FTP) Daemon is used as FTP server.

Deploying vsftp

Install the package

```
# yum install vsftpd
```

Start the server

```
# service vsftpd start
```

Enable the service to start at startup

```
# chkconfig vsftpd on
```

Open the firewall

```
# system-config-firewall-tui
```

Select customize enable **ftp** > ok

Test from remote machine

Syntax

```
# sftp < server IP address or hostname >
```

It will ask for username and password use linux username and password for server

To upload file on ftp prompt

```
sftp>put file_name
```

To download file

sftp> get file_name

To exit

sftp> bye

Example

```
[root@redhat2 ~]# sftp redhat1
Connecting to redhat1...
root@redhat1's password:
sftp> pwd
Remote working directory: /root
sftp> cd /etc/
sftp> pwd
Remote working directory: /etc
sftp> get hosts
```

```
Fetching /etc/hosts to hosts
/etc/hosts
100%   84    0.1KB/s   00:00
sftp> bye
```

Note You can connect to ftp server anonymously. You can download and upload files to /var/ftp directory.

To configure server to allow anonymous user users edit **/etc/vsftpd/vsftpd.conf**

Chapter 18

Web server

A webserver is program, which allows web browser clients to access web pages. it uses HTTP (Hypertext Transfer Protocol). In RedHat and derivatives Apache HTTP server is used.

Deploying http server

Install http server

```
# yum install httpd
```

Start service

```
# service httpd start
```

Enable the service to start on boot

```
# chkconfig httpd on
```

Default directory where http keeps contents

/var/www/html

Configuration file

/etc/httpd/conf/http.conf

Test

Create file in directory /var/www/html/index.html and Write **Hello**

Save the file and exit

Open the firefox on the address bar write http://localhost

You should see hello

Chapter 19

Firewall

According to dictionary, a firewall is a wall or partition designed to inhibit or prevent the spread of fire. In computers firewall is network security system that is used to secure the incoming and outgoing connections. It prevent unauthorized access to the system. It restrict user to access only designated services.

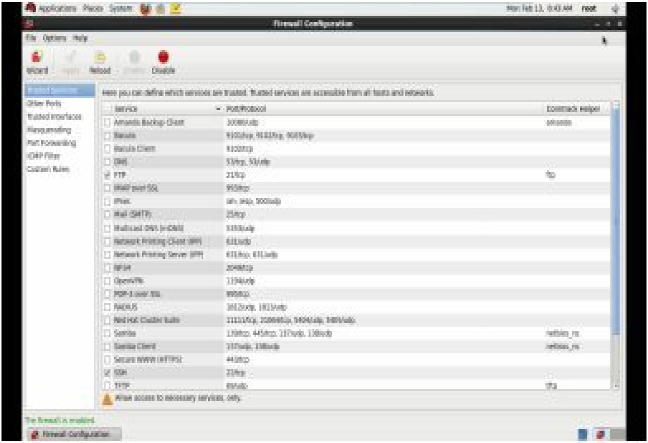
Redhat Linux kernel has built in firewall which can be used to allow or deny incoming and outgoing network traffic.

To configure firewall we have three ways to do that first is GUI mode, Second TUI mode and third manually:-

In GUI mode

```
# system-configure-firewall
```

Here you can enable or disable firewall. You can also allow or deny incoming and outgoing network. The main area of configuration is divided in to two pans left pan is category and right pan services and port numbers.



Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

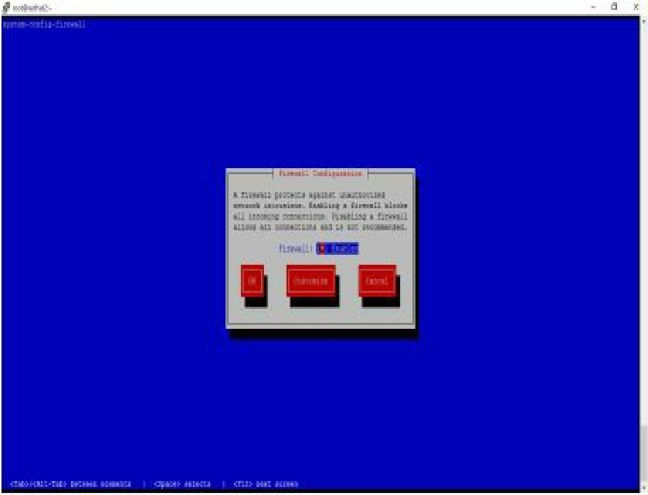
	Service	Port/Protocol	Conntrack Helper
□	Amanda Backup Client	10080/udp	amanda
□	Bacula	9101/tcp, 9102/tcp, 9103/tcp	
□	Bacula Client	9102/tcp	
□	DNS	53/tcp, 53/udp	
☑	FTP	21/tcp	ftp
□	IMAP over SSL	993/tcp	
□	IPsec	ah, esp, 500/udp	
□	Mail (SMTP)	25/tcp	
□	Multicast DNS (mDNS)	5353/udp	
□	Network Printing Client (IPP)	631/udp	
□	Network Printing Server (IPP)	631/tcp, 631/udp	
□	NFS4	2049/tcp	
□	OpenVPN	1194/udp	
□	POP-3 over SSL	995/tcp	
□	RADIUS	1812/udp, 1813/udp	
□	Red Hat Cluster Suite	11111/tcp, 21064/tcp, 5404/udp, 5405/udp	
□	Samba	139/tcp, 445/tcp, 137/udp, 138/udp	netbios_ns
□	Samba Client	137/udp, 138/udp	netbios_ns
□	Secure WWW (HTTPS)	443/tcp	
☑	SSH	22/tcp	
□	TFTP	69/udp	tftp

Allow access to necessary services, only.

The firewall is enabled.

In text mode

```
#system-config-firewall-tui
```



system-config-firewall

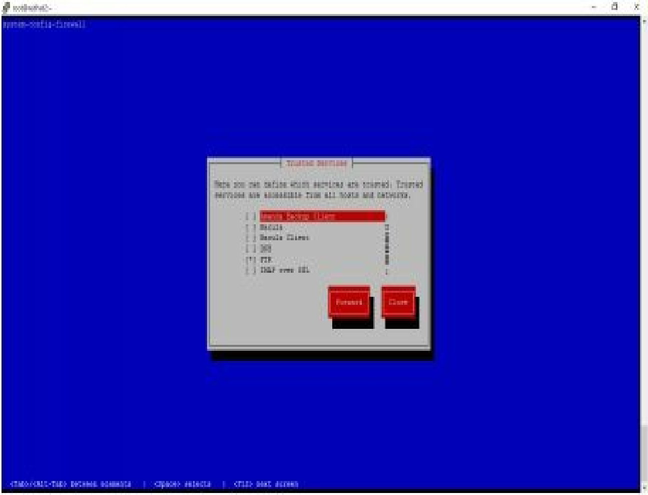
Firewall Configuration

A firewall protects against unauthorized network intrusions. Enabling a firewall blocks all incoming connections. Disabling a firewall allows all connections and is not recommended.

Firewall: [*] Enabled

OK
Customize
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Select **Enable** to enable firewall then press customize



```
system-config-firewall

                 ┤ Trusted Services ├
 Here you can define which services are trusted. Trusted
 services are accessible from all hosts and networks.

           [ ] Amanda Backup Client
           [ ] Bacula
           [ ] Bacula Client
           [ ] DNS
           [*] FTP
           [ ] IMAP over SSL

                                  Forward    Close

 <Tab>/<Alt-Tab> between elements   |  <Space> selects  |  <F12> next screen
```

Here you can configure which services and ports are trusted

Manual Configuration

Firewall configuration tool only configure basic firewall, if you need more granular configuration of firewall **iptable** and **ip6table** service provide the ability to configure firewall.

Configuration file

/etc/sysconfig/iptables

To display current rules

```
# iptables -L
```

Turn the firewall on

```
# service iptables start
```

Turn the firewall off

```
# service iptables stop
```

Save the configuration

```
# service iptables save
```

To open ports

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

or

```
iptables -A INPUT -p tcp --dport 22 -m
conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
```

- **dport** defines the port has be opened as ssh uses port 22 for communication.

- **-p tcp** defines the protocol being used

Similarly if you want to open http connection you have to open port 80

```
iptables -A INPUT -p tcp --dport 80 -m
conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -m
conntrack --ctstate ESTABLISHED -j ACCEPT
```

Rules created with iptables command as stored in memory it will not persist after system restart. To save the rules

```
# service iptables save
```

Or you can add manually in the

/etc/sysconfig/iptables file

Terms used in firewall

1. iptables
2. tables
3. chains
4. rules

The structure is iptables > Tables > chains >Rules

Chapter 20

Selinux

Selinux is **S**ecurity **E**nhanced **Linux**. Selinux is kernel module that improves the Linux server security. This is one of the solution for implementation of Access Control in Linux.

Selinux implements what is known as **MAC** Mandatory Access Control. Selinux is set of security rules which determine which process can access which file, directory or port etc. Selinux policy to access process, directoy , files is called as context. One goal of Selinux is to protect data and system. Selinux has three forms of access control:

1. Enforcing
2. Permissive
3. Disabled

Enforcing

Selinux denes access based on selinux policy rules.

Permissive

Selinux does not deny access but deniels are logged for the action that wouldd have been denied if running in enforcing mode.

Disabled

Selinux is completely disabled

Check the installation

```
# rpm -q | grep selinux
```

Check current mode

```
# getenforce
```

Check the status

```
# sestatus
```

Main configuration file

```
/etc/selinux/config
```

To Change the mode

Edit `/etc/selinux` configuration file and change **selinux=enforcing** to desired mode like **selinux= permissive**. After saving the file and reboot the server.

If you set the mode to **permissive** you can check the log what Selinux is doing.

```
# cat /var/log/messages |grep -i selinux
```

Or

```
tail -f /var/log/audit/audit.log
```

Commands to display context

Description	Command
List process conext	ps auxZ
Display user context	Id –Z
Display files with context	ls -lZ
copy wit context	cp -Z
mkdir with context	mkdir -Z

Install selinux

```
# yum install policycoreutil policycoreutil-
```

```
python
```

Tool to change context

```
# semanage
```

Show context

```
# semanage fcontext -1
```

Types

The main permission control method used in SELinux targeted policy to provide advanced process isolation is **Type Enforcement**. All files and processes are labeled as a type. Types define a SELinux domain for processes and a SELinux type for files

Example of Types are

httpd_sys_content_t

tmp_t

Add context

```
# semanage fcontext -a -t httpd_sys_content_t /abc/zzz.txt
# ls -Z
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 zzz.txt
```

Set the context to default

```
# restorecon -v -t /abc/zzz.txt
```

Booleans

Booleans allow a part of Selinux policy to change at runtime without any knowledge of Selinux policy writing

List Booleans

```
# semanage boolean -l
```

Configure Booleans

- list all

```
semanage boolean -l
```

- list Booleans weather they are on/off

```
getsebool -a
```

- Allow ftp read and write files in the users home directory

```
setsebool -P ftp_home_dir on
```

- Check

```
# getsebool ftp_home_dir
ftp_home_dir --> on
```

Chapter 21

Partition and file system

Partitions

Partition is to divide the storage, mostly hard disk into segments in which you can have more than one type of file systems. Partitioning of storage helps in managing storage properly.

fdisk is used to partition the disk.

List the partition table

```
fdisk -l
```

List the partition table for

specific

Syntax

fdisk -l <device name >

Example

```
fdisk -l /dev/hda1
```

Create new partition on device

In this example /dev/sda2 is added to system

First check the new device added

```
# fdisk -l
Disk /dev/sdb: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 =
8225280 bytes
Sector size (logical/physical): 512 bytes /
512 bytes
```

it will show the all storage device

Run fdisk on required device

```
fdisk -cu /dev/sdb
```

Check if partition is there on device selected with disk

Press **p** and **enter** key

```
Command (m for help): p

Disk /dev/sdb: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders,
total 41943040 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: 0xdec2ee90


  Device Boot      Start         End      Blocks
Id  System
```

Press **n** for new partition

Press **p** for primary

Give partition number like **1, 2, 3, 4**

Press **Enter** for starting section

For last sector, give size like +1G to create 1 GB partition

```
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (2048-41943039, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G}
(2048-41943039, default 41943039): +1G
```

Press **w** to write on disk

File system

File System is method used by operating system to store data and retrieve it. File system helps in managing and arranging data. File systems can be

- shareable
- non shareable

EXT File System

Extended file system (ext) is poplar file system used In Redhat. **Ext3** is journalized file system, it keeps track of changes not yet committed to the file system by recording such changes in data structure to journal which in turn generate circular log. In case of abrupt system down like power failure or crashed file system can be brought back online easily. There are different generation of **ext** File system

- ext2

- ext3
- ext4

.

ext2, ext3 came before RHEL 5 having limitation of file system size as 8TB /16TB and file size as 2 TB

Ext4 came in RHEL 5.6 file system and file size is 16TB. It is efficient reliable and robust.

Creating file system

Create partition with fdisk

fdisk -l check the device name

mkfs -t ext4 /dev/sdb1 where **sdb1** is device name and **ext4** is file system type

```
[root@redhat1 ~]# mkfs -t ext4 /dev/sdb1
mke2fs 1.41.12 (17-May-2010)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
65536 inodes, 262144 blocks
13107 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=268435456
8 block groups
32768 blocks per group, 32768 fragments
```

```
per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem
accounting information: done

This filesystem will be automatically
checked every 34 mounts or
180 days, whichever comes first.  Use
tune2fs -c or -i to override.
```

- **create mount point**

```
[root@redhat1 ~]# mkdir /test1
```

Add entry in the /etc/fstab

```
[root@redhat1 ~]# vi /etc/fstab


/dev/mapper/vg_redhat1-lv_swap swap
swap    defaults        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/cdrom      /cdrom                  iso9660
ro              0 0
/dev/sdb1       /test1                  ext4
```

```
default        0 2
```

Where **/dev/sdb1** is device **/test1** mount point, **ext4** for partition type, 0 for dump and 2 order for fsck.

Chapter 22

Swap space

Swap space is used in Linux and UNIX to free physical memory. The inactive pages of data is written to slower storage i.e. hard disk. The area where inactive data is written is called as swap space.

Add swap space

Create partition

```
[root@redhat1 ~]# fdisk /dev/sdb


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
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (307-6132, default 307):
Using default value 307
Last cylinder, +cylinders or +size{K,M,G}
(307-6132, default 6132): +1G
```

Change the type by pressing **t** of

partition slected to **82** which is **linux swap**

```
Command (m for help): t
Partition number (1-4): 2
Hex code (type L to list codes): 82
Changed system type of partition 2 to 82
(Linux swap / Solaris)
```

Check the partition

```
Command (m for help): p

Disk /dev/sdb: 21.5 GB, 21474836480 bytes
171 heads, 40 sectors/track, 6132 cylinders
Units = cylinders of 6840 * 512 = 3502080
bytes
Sector size (logical/physical): 512 bytes /
```

```
512 bytes
I/O size (minimum/optimal): 512 bytes / 512
bytes
Disk identifier: 0xdec2ee90

   Device Boot      Start         End      Blocks
Id  System
/dev/sdb1               1         307     1048576
83  Linux
/dev/sdb2             307         614     1050280
82  Linux swap / Solaris
```

Press w to write partition to disk

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

```
Calling ioctl() to re-read partition table.
Syncing disks.
```

mkswap /dev/sdb2 where sdb2 is name of the partition which will be used as swap.

```
[root@redhat1 ~]# mkswap /dev/sdb2
Setting up swapspace version 1, size =
1050276 KiB
no label, UUID=c1f98067-9548-4bf1-843d-
5f09f5d5ba56
```

Add entry in /etc/fstab

```
[root@redhat1 ~]# cat /etc/fstab
```

```
sysfs                   /sys                    sysfs
defaults       0 0
proc                    /proc                   proc
defaults       0 0
/dev/cdrom                  /cdrom
iso9660 ro          0 0
/dev/sdb1             /test1  ext4    default       0
2
UUID=c1f98067-9541-843-5f09f5d5ba56
swap  swap    defaults  0 0
```

swapon -a will activate swap

swapon -s will show status of all swap space

```
[root@redhat1 ~]# swapon -s
Filename                Type            Size    Used
```

```
Priority
/dev/dm-1           partition      2097144 0
-1
/dev/sdb2           partition      1050272 0
-2
```

To deactivate the swap space

```
# swapoff /dev/sdb2
```

Chapter 23

Logical Volume Manager

In earlier section we learned about creating Linux partition but we can also create partition type LVM (logical partition manager). When we create LVM type partition, LVM manages space allocated to it. Which is more sophisticated than normal Linux partition. LVM has following benefits

- Grow the File system dynamically
- shrink the File system

- Add disk dynamically
- Mirroring
- Stripping
- Snapshot as backup of File system

Terms used in LVM

Physical Volume

Physical Volume (PV) is physical storage unit of an LVM is a block device such as a partition or whole disk. To use the device for an LVM create partition with **fdisk** as **LVM** type.

Volume Groups

One or more physical volumes combined into Volume Group (VG).

Physical Extent

Storage space from Physical Volume is

divided in to small unit of fixed size known as physical extent, which is smallest unit that can be allocated. P.E. will same for all physical volume in the same VG.

Logical extent

Mapping of PE to make up front end of LVM. By default one PE is mapped to one LE But, you can map more than one PE to one LE in case of mirroring.

Logical Volume

Logical volume is group of Logical Extent. It is here we create File system.

Logical volume are not restricted to physical disk sizes. In addition, the hardware storage layer is isolated form software.

Steps to create File system with newly disk added to system

Create Physical volume (PV)

Use **fdisk** command and create partition type Linux LVM **8e**

```
[root@redhat1 ~]# fdisk /dev/sdb

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
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (615-6132, default 615):
Using default value 615
Last cylinder, +cylinders or +size{K,M,G}
(615-6132, default 6132): +5G

Command (m for help): t
Partition number (1-4): 3
Hex code (type L to list codes): 8e
Changed system type of partition 3 to 8e
(Linux LVM)
```

```
Command (m for help): p

Disk /dev/sdb: 21.5 GB, 21474836480 bytes
171 heads, 40 sectors/track, 6132 cylinders
Units = cylinders of 6840 * 512 = 3502080
bytes
Sector size (logical/physical): 512 bytes / 512
bytes
I/O size (minimum/optimal): 512 bytes / 512
bytes
Disk identifier: 0xdec2ee90

   Device Boot      Start         End      Blocks   Id
System
/dev/sdb1               1         307     1048576   83
Linux
/dev/sdb2             307         614     1050280
```

```
82  Linux swap / Solaris
/dev/sdb3            615        2148     5246280
8e  Linux LVM

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 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.
```

Reboot the server

Create PV using command **pvcreate *device_name*** where *device_name* is device created with fdisk

```
[root@redhat1 ~]# pvcreate /dev/sdb3
   Physical volume "/dev/sdb3" successfully
created
[root@redhat1 ~]# pvdisplay /dev/sdb3
  "/dev/sdb3" is a new physical volume of "5.00
GiB"
  --- NEW Physical volume ---
  PV Name               /dev/sdb3
  VG Name
  PV Size               5.00 GiB
  Allocatable           NO
  PE Size               0
```

```
 Total PE          0
 Free PE           0
 Allocated PE        0
 PV UUID             EQ7ElZ-WiGK-Z0m5-
5gSN-gP95-MFSk-pKyTvS
```

Create Volume Group (VG)

vgcreate ***VG_name PV_name***

```
[root@redhat1 ~]# vgcreate vg01 /dev/sdb3
 Volume group "vg01" successfully created
```

Create new Logical Volume(LV)

lvcreate -n ***LV_name*** **-L** ***size VG_name***

```
[root@redhat1 ~]# lvcreate -n lv01 -L 1G vg01
 Logical volume "lv01" created
```

Create File System on LV

mkfs -t ext4 /dev/*VG_name*/*LV_name*

```
[root@redhat1 ~]# mkfs -t ext4 /dev/vg01/lv01
```

Add entry to **/etc/fstab** mount system automatically at startup

```
UUID=6acaa400-0cd3-4708-ba05-
5541139e830e  /newfs      ext4    defaults
1 2
```

Mount the file system

mount -a

PV Commands

Description	Command

Display PV properties	pvdisplay
Show all LVM block devices	pvscan
Prevent allocation of PE on PV	pvchange -xn */dev/PV_name*
Remove PV	pvremove */dev/PV_name*

Volume Group Commands

Description	**Command**
Display VG properties	vgdisplay
Display VG List	vgs

Add PV to VG	vgextend vgname */dev/PV_name* **Example** # vgextend vg01 /dev/sdb5
Remove PV form VG	vgreduce vg1 */dev/PV_name* **Example** # vgreduce vg01 /dev/sdb5
Activating VG	vgchange -ay *VG_name*
deactivating VG	vgchange -ay *VG_name*
Remove VG	vgremove *VG_name*

	Example `vgremove /dev/vg02`
Recreate a VG Directory	vgmknodes

Moving Volume group from one system to other

On first system where VG is currently running unmount all FS which is part of VG

```
umount /newfs
```

Deactivate the VG **vgchange -an *VG_name*** command

```
[root@redhat1 /]# vgchange -an sharedvg
```

Export the VG with **vgexport *VG_name*** command

```
[root@redhat1 /]# vgexport sharedvg
```

After attaching HDD to new system import the VG with **vgimport *VG_name*** command

```
[root@redhat2 ~]# vgimport sharedvg
```

Activate the VG with **vgchange -ay VG_name**

```
[root@redhat2 ~]# vgchange -ay sharedvg
```

Mount the file systems on the VG

```
[root@redhat2 ~]# mount
/dev/sharedvg/sharedlv /mnt
```

Check the contents of file system

```
[root@redhat2 ~]# cd /mnt
```

Extending FileSystem

Check the current FS size

df -h /fsname

```
/dev/mapper/vg01-lv01        1008M   34M
924M   4% /newfs
```

Check if you have enough free space i.e free PE on the VG where LV of FS you want extend is there.

```
[root@redhat1 ~]# vgdisplay vg01
 --- Volume group ---
 VG Name               vg01
 System ID
 Format                lvm2
 Metadata Areas        1
 Metadata Sequence No  5
 VG Access             read/write
 VG Status             resizable
 MAX LV                0
 Cur LV                1
 Open LV               1
 Max PV                0
 Cur PV                1
 Act PV                1
 VG Size               5.00 GiB
 PE Size               4.00 MiB
 Total PE              1280
 Alloc PE / Size       256 / 1.00 GiB
 Free  PE / Size       1024 / 4.00 GiB
 VG UUID               EXKfhW-MfE4-4ZtU-
uQuM-v9e4-AJ9k-Uo6z4B
```

Extend the Logical Volume **lvextend -L size /dev/vgname/lvname**

```
[root@redhat1 ~]# lvextend -L +200M
/dev/vg01/lv01
  Extending logical volume lv01 to 1.20 GiB
  Logical volume lv01 successfully resized
```

Extend the file system using **resize2fs -p /dev/vgname/lvname**

```
[root@redhat1 ~]# resize2fs -p
/dev/mapper/vg01-lv01
```

Check the FS size **df -h /fsname**

```
/dev/mapper/vg01-lv01       1.2G   34M  1.1G
3% /newfs
```

Reduce the File System

Check the current FS size

df -h /fs_name

```
/dev/mapper/vg01-lv01       1.2G   34M  1.1G
3% /newfs
```

unmount the Filesystem

umount /fs_name

```
 [root@redhat1 ~]# umount /newfs
```

Check the file system

```
[root@redhat1 ~]# e2fsck -f
/dev/mapper/vg01-lv01
```

Resize FS

resize2fs -p /dev/vgname/lvname size

```
[root@redhat1 ~]# resize2fs -p
/dev/mapper/vg01-lv01 1G
```

In this example make the size of FS as 1 GB

Now reduce the LV size keep some extra space than filesytem

lvreduce -L size /dev/vgname/lvname

```
[root@redhat1 ~]# lvreduce  -L 1.1G
/dev/mapper/vg01-lv01
```

Mount File system

mount /fs_name

```
[root@redhat1 ~]# mount /newfs
```

Chapter 24

LVM snapshot

LVM snapshot is a point in time copy of Logical Volume. The snapshot provides static view of original volume. Once snapshot has been taken we can use this snapshot to take backup volume as snapshot is static copy and it will not change while backup is happening unlike the original volume which is dynamic.

The snapshot volume size should be enough to store the data that will change after snapshot has been taken. the volume will store only changes after the snapshot has been taken.

Create snapshot LV

Check the LV name and size of File System for which you want to create snapshot

```
[root@redhat1 /]# df -hT /newfs
Filesystem       Type  Size  Used Avail Use%
Mounted on
/dev/mapper/vg01-lv01 ext4 1008M   34M
924M   4% /newfs
```

Check you have space at least equivalent to 10% of file system you want to take snapshot available on the VG where original LV is located

```
# vgdisplay vg01
```

Create LV 8 to 10 % of capicity of original LV

lvcreate -s -n snaplvname -L size /dev/vgname/orginal_lv_name

```
# lvcreate -s -n snaplv1 -L 100M
/dev/mapper/vg01-lv01
```

if you want to see content of snapshot LV

mount -o ro /dev/vgname/snaplv /mount_point_snaplv

```
# mount -o ro /dev/vg01/snaplv1 /snapfs/
```

Change to directory to check the contents

cd /mount_point_snaplv

```
cd /snapfs/
ls
```

Remove snapshot LV

Unmount snap File system

umount /mount_point_snaplv

```
[root@redhat1 /]# umount /snapfs
```

Remove the snap logical

lvremove /dev/vgname/snaplv

```
[root@redhat1 /]# lvremove /dev/mapper/vg01-snaplv1
```

Chapter 25

Boot process

Boot process of Linux

1. **BIOS**
2. **Master Boot Record**
3. **GRUB**

   Uses /boot/grub/grub.conf to select the kernel image.
4. **Kernel**
   1. Mounts the root file system as specified in the “root=” in grub.conf
   2. **Kernel executes the /sbin/init program which is the first**

program executed by the kernel

3. **initrd stands for Initial RAM Disk. initrd is used by kernel as temporary root file system until kernel is booted and the real root file system is mounted. It also contains drivers which are required to access hard disk and other necessary hardware.**

5. **Init**

   It reads /etc/inittab file to decide the Linux run level.

Following are the available run levels

0 – halt

1 – Single user mode

2 – Multi user mode without network

3 – Full multiuser mode

4 – unused

5 – GUI

6 – reboot

Typically you would set the default run level to either 3 or 5.

6. Runlevel

Depending on Runlevel selected by inittab some services will start other will stop, the system will execute the programs from one of the following directories.

Run level 0	/etc/rc.d/rc0.d/
Run level 1	/etc/rc.d/rc1.d/
Run level 2	/etc/rc.d/rc2.d/
Run level 3	/etc/rc.d/rc3.d/

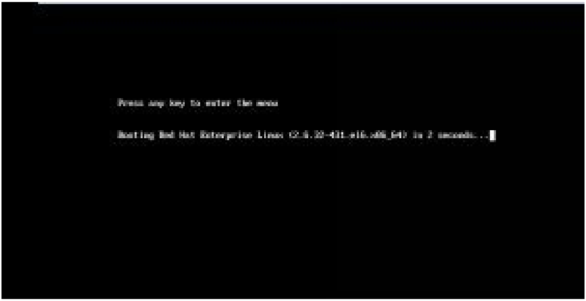
Run level 4	/etc/rc.d/rc4.d/
Run level 5	/etc/rc.d/rc5.d/
Run level 6	/etc/rc.d/rc6.d/

Under the /etc/rc.d/rc*.d/ directories, you would see programs that start with S and K which are symbolic link to actual scripts in /etc/rc.d/init.d/ directory. There are numbers right next to S and K in the program names. Those are the sequence number in which the programs should be started or killed. For example, S82sendmail is to start the sendmail daemon at sequence number of 82.

Chapter 26

Reset unknown root password

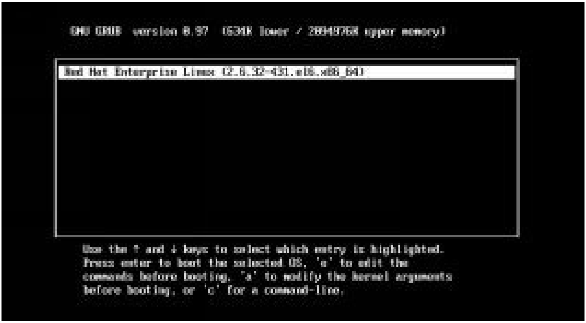
1. At menu press any key any key to enter GRUB menu



```
Press any key to enter the menu

Booting Red Hat Enterprise Linux (2.6.32-431.el6.x86_64) in 2 seconds...
```

2. At GRUB menu press **a**

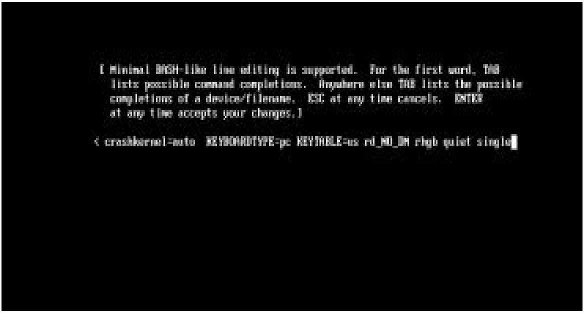


```
    GNU GRUB  version 0.97  (634K lower / 2094976K upper memory)

 Red Hat Enterprise Linux (2.6.32-431.el6.x86_64)

      Use the ↑ and ↓ keys to select which entry is highlighted.
      Press enter to boot the selected OS, 'e' to edit the
      commands before booting, 'a' to modify the kernel arguments
      before booting, or 'c' for a command-line.
```

3. Add single at the end of line

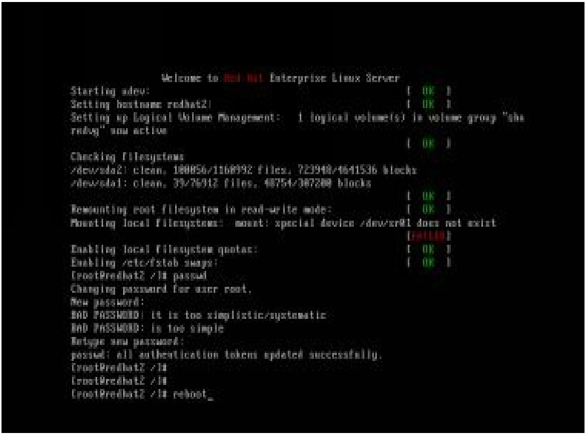


```
   [ Minimal BASH-like line editing is supported.  For the first word, TAB
     lists possible command completions.  Anywhere else TAB lists the possible
     completions of a device/filename.  ESC at any time cancels.  ENTER
     at any time accepts your changes.]

  < crashkernel=auto  KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb quiet single
```

4. press enter

5. At # prompt write **passwd** give new password and reboot the system



```
                 Welcome to Red Hat Enterprise Linux Server
Starting udev:                                             [  OK  ]
Setting hostname redhat2:                                  [  OK  ]
Setting up Logical Volume Management:   1 logical volume(s) in volume group "sha
rodvg" now active
                                                           [  OK  ]
Checking filesystems
/dev/sda2: clean, 100056/1160992 files, 723940/4641536 blocks
/dev/sda1: clean, 39/76912 files, 40754/307200 blocks
                                                           [  OK  ]
Remounting root filesystem in read-write mode:             [  OK  ]
Mounting local filesystems:  mount: special device /dev/sr01 does not exist
                                                           [FAILED]
Enabling local filesystem quotas:                          [  OK  ]
Enabling /etc/fstab swaps:                                 [  OK  ]
[root@redhat2 /]# passwd
Changing password for user root.
New password:
BAD PASSWORD: it is too simplistic/systematic
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
[root@redhat2 /]#
[root@redhat2 /]#
[root@redhat2 /]# reboot_
```

6. After reboot the system will have new root password

6.

Chapter 27

Identify your system

Know version of Redhat

```
# /etc/redhat-release
```

or

```
# lsb-release
```

Know running kernel version

```
# uname -r
```

or

```
# cat /proc/version
```

List all installed kernel

version

```
# yum list installed kernel\*
```

Display CPU information

```
# lscpu
```

or

```
# cat /proc/cpuinfo
```

List all PCI devices

```
# lspci
```

Detailed description of system hardware

```
# dmidecode
```

Display memory

information

```
# cat /proc/meminfo
```

or

```
# free -m                    shows memory in MB
```

List block device

```
# lsblk
```

List all partitions

```
# fdisk -l
```

List CPU, Memory, Process

```
# top
```

Display Hostname

```
# hostname
```

sosreport

The "**sosreport**" is a tool to collect troubleshooting data on RHEL/CentOS systems. It generates report of configuration of Linux system and most important logs in tarball compressed format which can be sent to Redhat for support related to any problem or performance issues.

Install package

```
# yum install sos
# yum install abrt-cli
```

Generate report

```
# sosreport
```

It prompts for the name of file and logged case number for which you are generating report. If you do not have case number.