

ESSENTIALS OF RED HAT LINUX

Session 13

Networking



Objectives



- Explain the features available for basic administration
- Explain network tasks such as printing and Web browsing
- Explain system monitoring
- Explain the concepts of network
- Explain the process of configuring remote hosts
- Explain the process of deploy an file sharing service
- Explain NFS
- Configure NFS and explain autofs



- If there are two or more computers connected together, it is considered to be a network.
- RHEL uses Common UNIX Printing System (CUPS) as the default printing system.
- CUPS use the Internet Printing Protocol (IPP) for broadcasting the shared printers and allow other users to use this information to connect to the shared printers.
- The other users on the network can browse through the shared printers.
- The remote computers that are connecting to the shared printers do not require printer configuration.
- The shared printers that other computers connect to are shown under the Remote Printers section in Printer Configuration.

Managing Printers



The three ways in which printers can be managed are:

- By editing the `printers.conf` configuration file in the `/etc/cups` directory. This file can be modified to allow only a few printers to the public.
- By using the Printer Configuration tools that can be invoked from the System → Administration → Printing.
- By invoking the `system-config-printer` tool from the command prompt.

Printers can be added to the computer in two ways:

- **Individual printer:** A single printer is added to the computer. If the printer goes offline or is unavailable, the computer is unable to print.
- **Printer class:** A group of printers are added to the computer as a single printer. The class can have both local and remote printers.

Web Browser



- Mozilla Firefox is the default Web browser for the RHEL operating system. The pre-installed version with RHEL is 3.6.9.

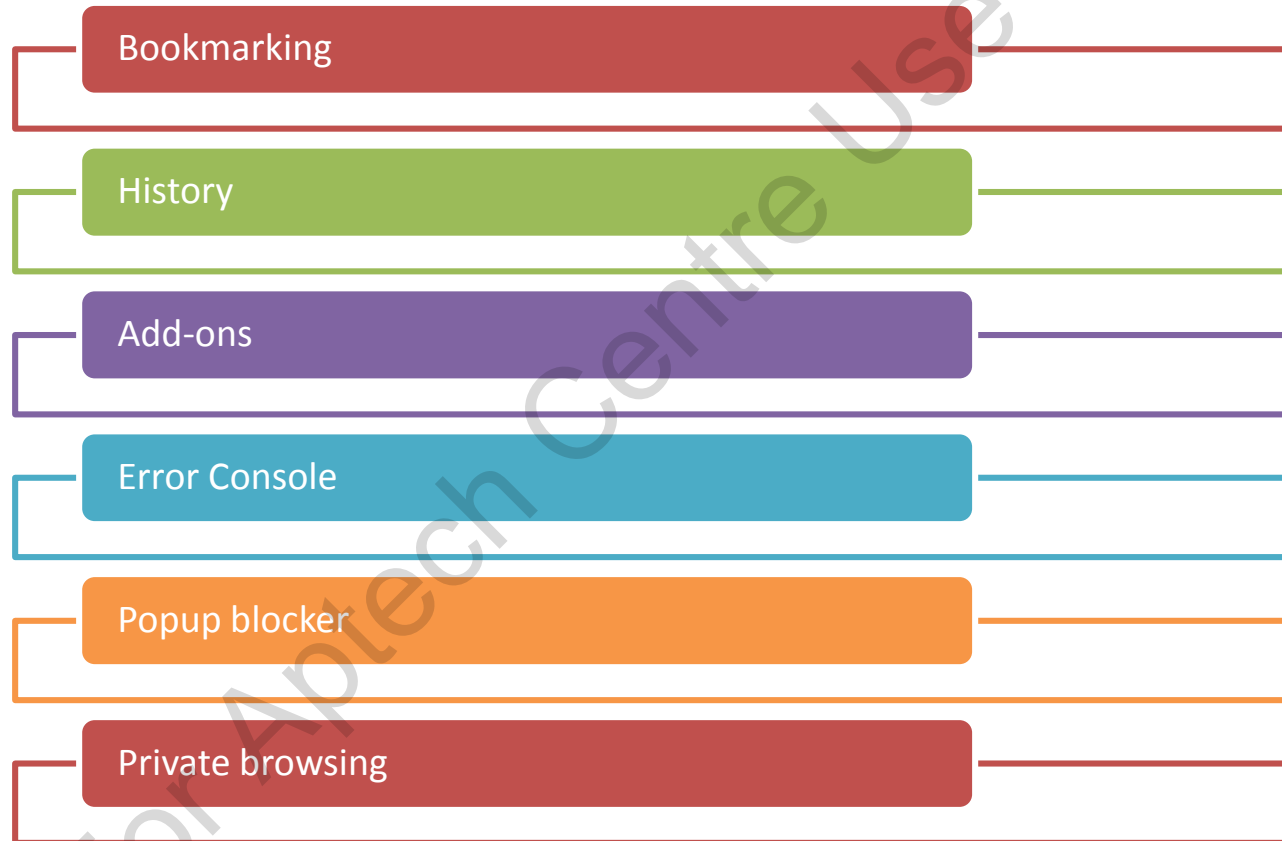


Mozilla Firefox

Features of Mozilla Firefox



- Some of the features of Mozilla Firefox are:



System Monitor [1-5]



RHEL allows users to manage and monitor system using the System Monitor, which can be accessed from the **Applications → System Tools** menu.

A user can use the System Monitor to:

- Keep a watch over the processes that are running
- Resources that are being utilized
- File system status, such as free space

The key system resources are:

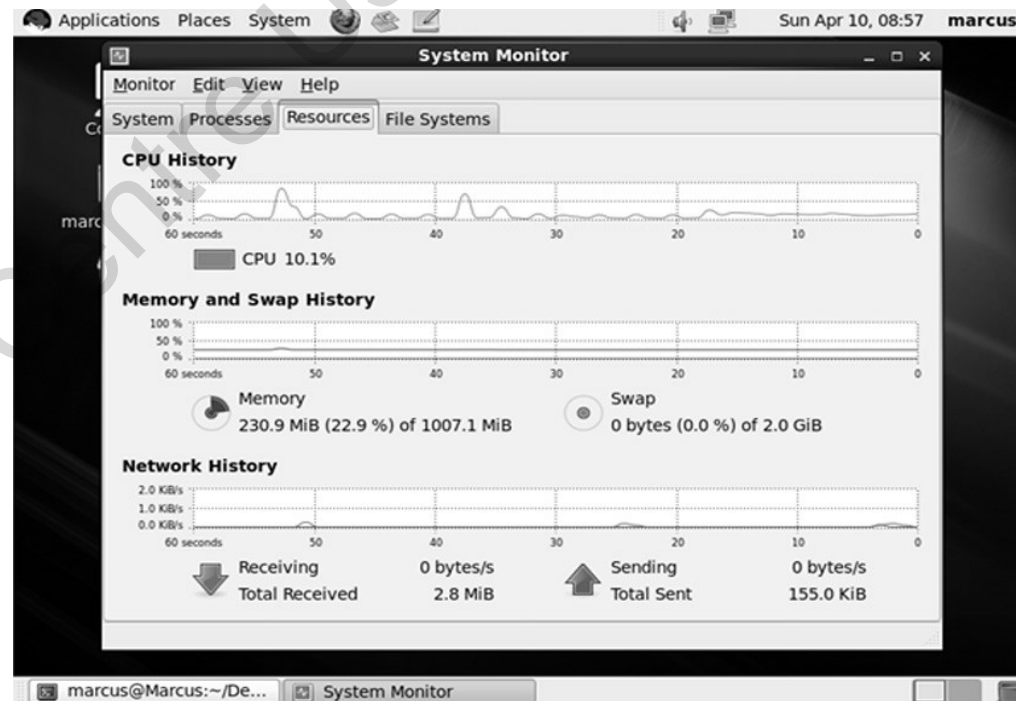
- The CPU
- Memory
- Network
- Disk

Monitoring and managing system resources at regular intervals is very essential for a system administrator.

System Monitor [2-5]



- In the System Monitor, the Resources tab shows the following key resources that are being monitored:
 - CPU usage
 - Memory and Swap file usage
 - Network usage

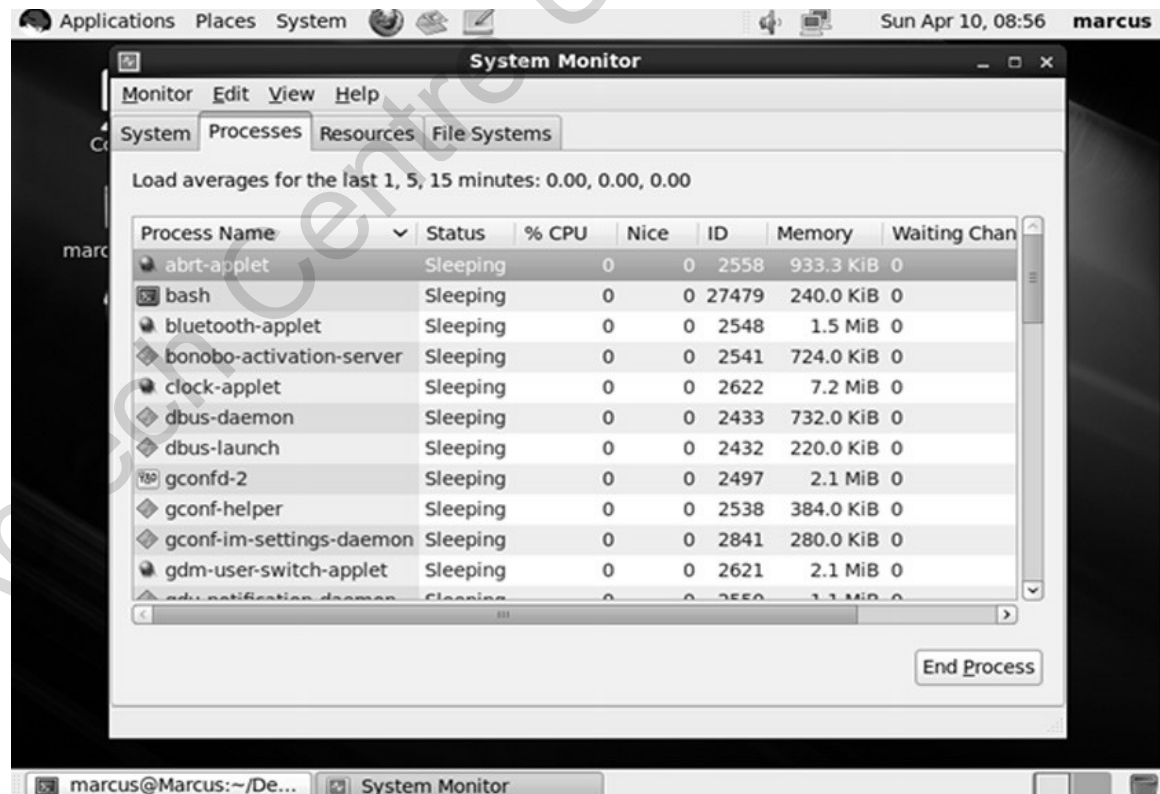


Resources Tab



System Monitor [3-5]

- The Processes tab displays the list of running processes.
- Using this tab, the user can:
 - Change the priority of a process
 - Kill a process
 - Start/Stop a process

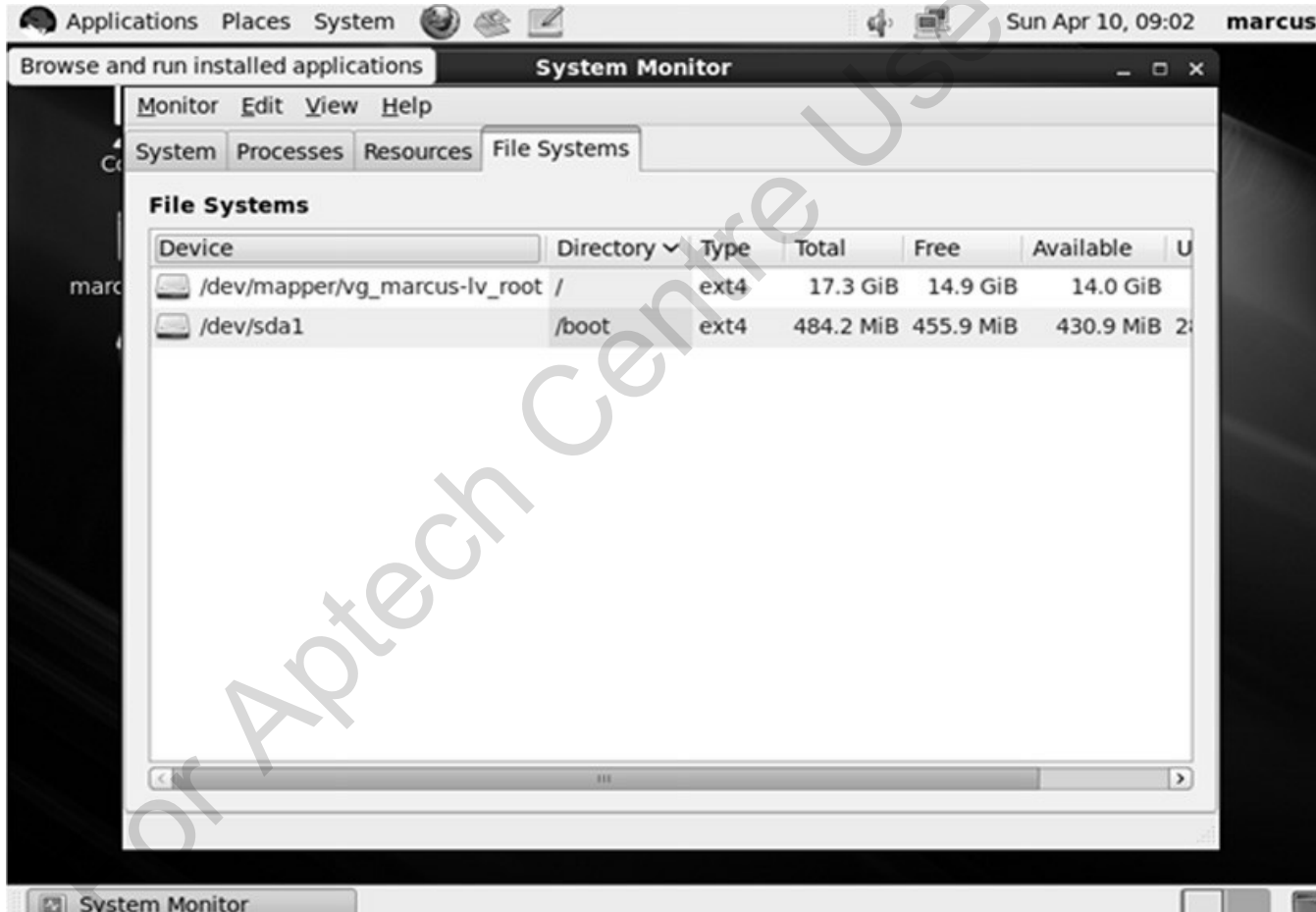


Processes Tab

System Monitor [4-5]



- The File Systems tab displays the status of the available file systems.



File Systems Tab



System Monitor [5-5]

- A user can also check the status of the processes from the command prompt using the `top` command. To view the current processes, type `top` at the command prompt.

```
top - 09:27:08 up 4:49, 2 users, load average: 0.00, 0.00, 0.00
Tasks: 138 total, 1 running, 137 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.3%us, 0.3%sy, 0.0%ni, 99.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 1031320k total, 932124k used, 99196k free, 71840k buffers
Swap: 2064376k total, 0k used, 2064376k free, 628456k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1188	dbus	20	0	14860	1924	996	S	0.3	0.2	0:02.44	dbus-daemon
2339	root	20	0	49988	20m	8592	S	0.3	2.1	0:47.81	Xorg
1	root	20	0	2824	1408	1204	S	0.0	0.1	0:01.70	init
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	migration/0
4	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
5	root	RT	0	0	0	0	S	0.0	0.0	0:00.00	watchdog/0
6	root	20	0	0	0	0	S	0.0	0.0	0:00.07	events/0
7	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuset
8	root	20	0	0	0	0	S	0.0	0.0	0:00.00	khelper
9	root	20	0	0	0	0	S	0.0	0.0	0:00.00	netns
10	root	20	0	0	0	0	S	0.0	0.0	0:00.00	async/mgr
11	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pm
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	sync_supers
13	root	20	0	0	0	0	S	0.0	0.0	0:00.00	bdi-default
14	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kintegrityd/0
15	root	20	0	0	0	0	S	0.0	0.0	0:00.78	kblockd/0

Output of the `top` command

Managing System Software [1-2]



- Software updates can be applied to the RHEL operating system either locally or through the RHN Web site.
- `yum` helps in uploading the software updates to the RHEL operating system.
- It can be configured to receive updates from software repositories that are located on the Internet or an intranet.
- A user must be logged on as a root user to run the `yum` command.
- `yum` has a number of advantages that help in providing software updates and they are:

Provides updates according to the hardware architecture or software version.

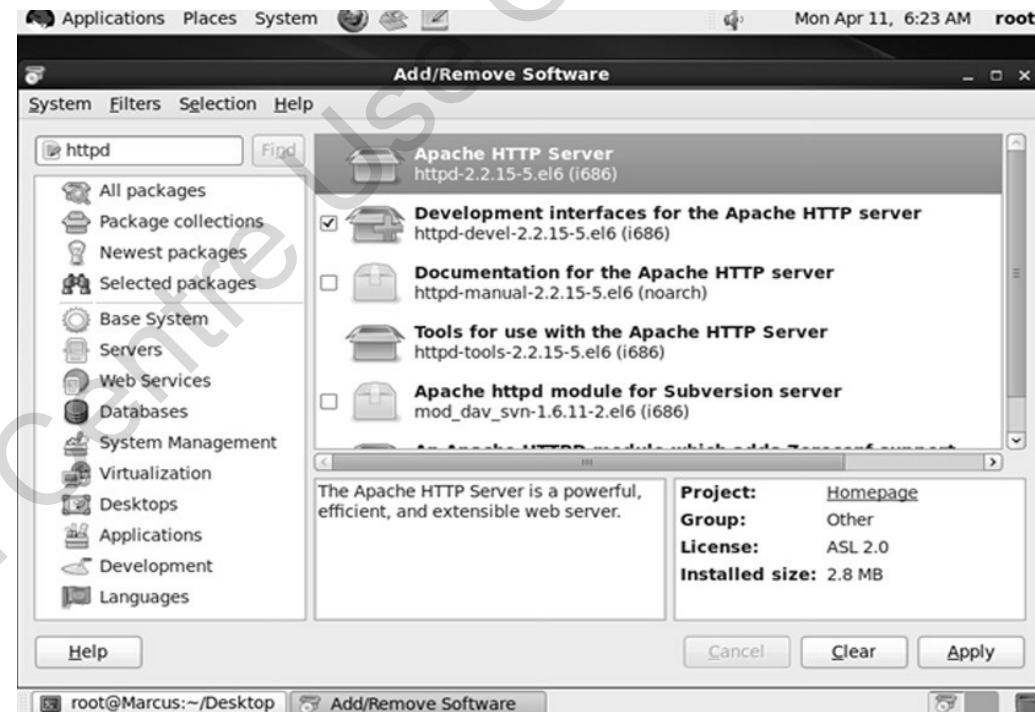
Fetches software updates from various locations.

Available in two different formats, graphical and command line.

Managing System Software [2-2]



- To run the updates from the command prompt, execute the following command:
`#yum install <pkgname>`
- A user can choose to install either specific hardware architecture or a particular version of the application.
- A user can also perform software updates from the graphical interface. A user can use the Add/Remove Software utility that can be invoked from **System → Administration**.



Add/Remove Software Utility Window

Establishing Network Connectivity



- There are three different methods to establish network connectivity. The following tasks can be performed by the users:

Add a new network adapter

Modify the existing network adapter properties

Assign an IP address to the network adapter

Assign or change DNS server

- The different methods used to configure the network are:

Configuring network at the command prompt

Configuring network in graphical environment (X Window System or GUI tool)

Configuring network configuration files

Administering Remote Systems



- RHEL provides multiple tools to remotely manage computers that can be located far from where the administrator is located. Some of the tools are as follows:

Secure Shell

Rsync

Nautilus

For Apteck Centre Use Only

Secure Shell



- Secure Shell (SSH) is part of the OpenSSH suite of tools that are included in the RHEL operating system.
- There are two components in OpenSSH:

Sever

- The computer that is being connected.

Client

- The computer that is initiating the action to the server.

- The *ssh* command is as follows:

```
ssh [user@]hostname
```

```
ssh [user@]hostname [command]
```


Rsync [1-2]



Rsync:

A utility that helps in backing up data on local and remote computers

Used to:

- Copy data from local computers to the remote computers.
- Copy data between two directories on a local computer.

Advantage: Only copies the difference between the files if there is any duplicity.

```
Usage: rsync [OPTION]... SRC [SRC]... DEST
or  rsync [OPTION]... SRC [SRC]... [USER@]HOST:DEST
or  rsync [OPTION]... SRC [SRC]... [USER@]HOST::DEST
or  rsync [OPTION]... SRC [SRC]... rsync://[USER@]HOST[:PORT]/DEST
or  rsync [OPTION]... [USER@]HOST:SRC [DEST]
or  rsync [OPTION]... [USER@]HOST::SRC [DEST]
or  rsync [OPTION]... rsync://[USER@]HOST[:PORT]/SRC [DEST]
```

rsync **Command**

Rsync [2-2]



- The parameters for the rsync command are:

Options

- Parameters passed to the command

First directory

- Source directory from which files must be backed up

Second directory

- Destination directory to which the files should be backed up

- An example of rsync command is as follows:

```
rsync -avz /home test1.abc.com:backup_storage/
```

Nautilus



- Nautilus:
 - Is a multipurpose utility that allows connecting to a remote computer.
 - Offers SSH as a service that can be used for connecting to a remote computer.



The image shows a 'Connect to Server' dialog box. It has a title bar with a folder icon and a close button. The 'Service type' dropdown is set to 'SSH'. The 'Server' field contains 'fileserver1'. Below this is a section for 'Optional information' with five empty text fields for 'Port', 'Folder', 'User Name', and 'Name to use for connection'. At the bottom are four buttons: 'Help' (with a question mark icon), 'Browse Network', 'Cancel' (with an 'X' icon), and 'Connect'.

Nautilus SSH Dialog Box

Deploying File Sharing Services [1-3]



- FTP follows client-server architecture in which one computer acts as the server and other computer acts as the client.
- The client computer connects to the server computer and initiates a request to either upload or download files.
- The server computer, which is known as the FTP server, accepts the incoming connections from the sending computer, which is known as the FTP client.
- The default FTP server for the RHEL operating system is Very Secure FTP Daemon (vsftpd).
- The key configuration file in which FTP related configuration is stored is `vsftpd.conf`. The file is located in the **/etc/ vsftpd** directory.

For Apteck Certified Users Only

Deploying File Sharing Services [2-3]



- Users can configure the following parameters in the `vsftpd.conf` file:

`listen_port`

- Contains the default value as 21, which is the port that FTP server would use.

`ftpd_banner`

- Defines the banner. This is the welcome message after the user logs on to the FTP server.

`local_enable`

- Contains the default value as NO, which indicates that the local users are not allowed to log on to the FTP server.

`hide_ids`

- Contains the default value as NO.

`max_clients`

- Contains the default value as 0, which indicates unlimited number of connections.



Deploying File Sharing Services [3-3]

- RHEL provides a tighter control over the anonymous connections. The `vsftpd.conf` file provides a number of configurable parameters as follows:

```
anonymous _ enable
```

```
allow _ anon _ ssl
```

```
anon _ mkdir _ write _ enable
```

```
anon _ other _ write _ enable
```

```
anon _ world _ readable _ only
```

```
deny _ email _ enable
```

```
no _ anon _ password
```

Allowing or Denying User Connections



Allowing a connection

- The `user_list` file stored in the `/etc/vsftpd` directory is used.
- This file is applicable only when users enable the `userlist_enable` directive in the `vsftpd.conf` file.
- The `userlist_deny` parameter must be set to `NO` to allow the users in the `userlist` to connect to the FTP server.

Denying a connection

- Users can use the `ftpusers` file stored in the `/etc/vsftpd` directory.
- This file contains two users by default, `root` and `nobody`.

Configuring a Web Server [1-2]



- FTP server follows a client-server model.
- The FTP server is meant for uploading and downloading files and the Web server is meant to serve Web pages to the clients.
- Web server has the following two key components:
 - Web server
 - Client
- RHEL can be configured with Apache Web server that mainly uses two different protocols:
 - TCP
 - UDP
- The default port that is used by HTTP is port 80.
- To configure a Web server, users must download and install the httpd package from the Red Hat Network.

Configuring a Web Server [2-2]



- After the server is installed, users must configure the `httpd.conf` file that is located in the `/etc/httpd` directory.
- There are three key sections in this file that are as follows:

Global Configuration

- Contains the global configuration values, such as `ServerRoot`, `KeepAlive`, and `Listen`.

Main Server

- Contains the server specific parameters, such as `ServerAdmin`, `ServerName`, and `DocumentRoot`.

Virtual Hosts

- Allows users to configure more than one Web site in the form of virtual hosts.

Starting and Stopping the Web Server



- To start and stop the Web server, a user must be a root user.
- Following command must be executed to start the Web server:

```
service httpd start
```

- Following command should be executed to stop the Web server:

```
service httpd stop
```

For Aptech Centre Use Only



- NFS is a server-client protocol that allows sharing of files between computers which are located on a common network.
- NFS is available on a variety of Linux and UNIX platforms.
- The client must use a NFS server compatible client application to be able to connect to the NFS server.
- NFS is available in different versions. RHEL supports the following versions:
 - NFSv2
 - NFSv3
 - NFSv4
- By default, RHEL uses NFSv4, which has the capability to work through firewalls.
- It also supports Access Control Lists (ACLs) and stateful operations.
- It requires Transmission Control Protocol (TCP) that is running over the IP network.

Advantages of NFS



NFS makes file sharing simple and effortless. The advantages of NFS are:

The server and client can use different operating systems.

The client mounts the remote directories to local directories.

Access is granted to the client IP address and therefore, no user authentication is required.

Connecting NFS Client and Server



- The steps used to connect the NFS Client and Server are:

1. The NFS server exports a directory to the client system as requested.

2. The client system mounts the directory to a local directory. This is called a mount point.

3. The Input/Output (I/O) operations are written to the server.

4. Client recognizes the changes as if they are being performed on the local directories, rather than the remote directories.

Configure NFS



- To be able to use the NFS shares on the server, the client must mount the shares first. Following command is used to mount the shares:

```
mount
```

- Editing and adding a line in the **/etc/fstab** file is a method to mount an NFS share.
- The user must be a root user to modify this file.
- Following syntax is used to add a line to the **/etc/fstab** file:

```
server:/remote/export /local/directory nfs options 0 0
```
- Following parameters must be contained in the command:
 - Hostname of the NFS share
 - Directory that is being exported from the server
 - Directory on which share is being mounted on the local machine



Autofs Service [1-3]

- Used to monitor preconfigured NFS mount points. It uses the automount daemon for this.
- The two components in the automount utility are:

Kernel Module

- Implements a file system

User-space Daemon

- Performs different functions.

- The file systems supported by automount are:

Andrew File System (AFS)

Samba File System (SMBFS)

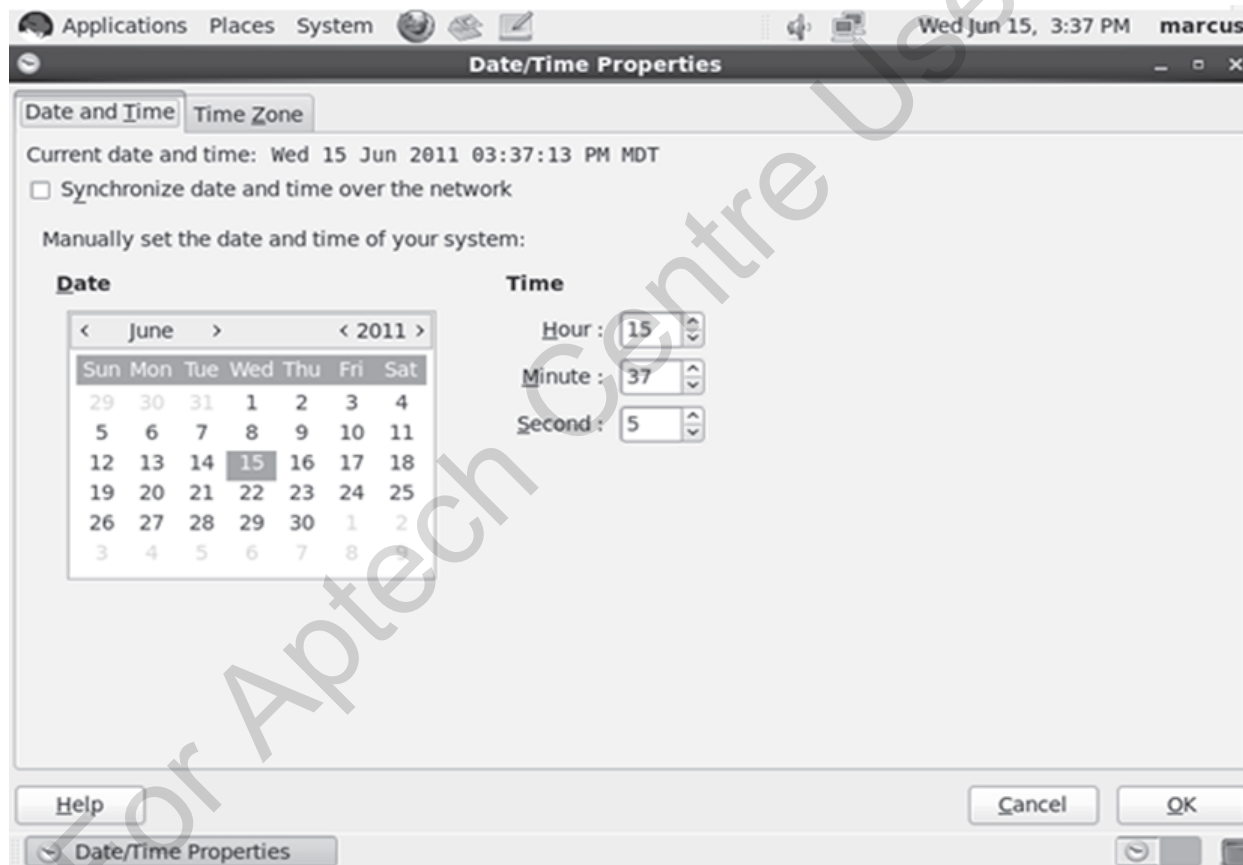
Common Internet File System (CIFS)

Local File Systems

Autofs Service [2-3]



- The autofs service uses the **/etc/auto.master** file as the default configuration file.



Sample auto.master File

Autofs Service [3-3]



- The auto.master file uses a redirection for the mounts to the **/misc/** directory. The redirection is mapped to the **/etc/auto.misc** file.



auto.misc Redirection

Starting the automount Daemon [1-2]



- To start the automount daemon, the system administrator must execute the following command:

```
service autofs start
```

A screenshot of a Linux desktop environment. At the top is a menu bar with 'Applications', 'Places', and 'System'. Below it is a panel with system icons and the date/time 'Sat Apr 30, 8:31 AM' and the user name 'Marcus Caesar'. A terminal window is open, titled 'root@localhost:~'. The terminal shows the user switching to root with 'su - root', entering a password, and then running 'date', which outputs 'Sat Apr 30 08:31:05 EDT 2011'.

```
Applications Places System Sat Apr 30, 8:31 AM Marcus Caesar
Browse and run installed applications root@localhost:~
File Edit View Search Terminal Help
[Caesar@localhost ~]$ su - root
Password:
[root@localhost ~]# date
Sat Apr 30 08:31:05 EDT 2011
[root@localhost ~]#
```

Starting the autofs Service

Starting the automount Daemon [2-2]



- To stop the automount daemon, the system administrator must use the command as follows:

```
service autofs stop
```

A screenshot of a Linux terminal window. The window title bar shows 'Applications Places System' and the user 'Marcus Caesar' on 'Sun May 1, 6:00 PM'. The terminal prompt is 'root@localhost:~'. The user has executed 'su - root' and entered the password. They then run 'date', which shows 'Sat Apr 30 08:31:05 EDT 2011'. Next, they run 'date -s "1 MAY 2011 18:00:00"', which updates the time to 'Sun May 1 18:00:00 EDT 2011'. The prompt is now '[root@localhost ~]#'.

```
root@localhost:~  
File Edit View Search Terminal Help  
[Caesar@localhost ~]$ su - root  
Password:  
[root@localhost ~]# date  
Sat Apr 30 08:31:05 EDT 2011  
[root@localhost ~]# date -s "1 MAY 2011 18:00:00"  
Sun May 1 18:00:00 EDT 2011  
[root@localhost ~]#
```

Stopping the autofs Service

Exercise 1 [1-7]



Viewing the `auto.master` file

Step 1

- Log on to the RHEL workstation using root username and password.

- User must have root permission to edit the `rsyslog.conf` file. All other users should have read permissions.

For Aptech Centre Use Only

Exercise 1 [2-7]



Step 2

- On the desktop, double-click **Computer**.

A screenshot of a Linux terminal window. The window title is 'Caesor@localhost:~/Documents'. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal text shows the user running 'ls' and 'cd Documents'. The desktop background is visible behind the terminal window.

```
Caesor@localhost:~/Documents
File Edit View Search Terminal Help
[Caesor@localhost ~]$ ls
data1 Desktop Documents Music Public Videos
data1~ Document Downloads Pictures Templates
[Caesor@localhost ~]$ cd Documents
```

Computer Icon

Exercise 1 [3-7]



Step 3

- Double-click Filesystem and open the **/etc/ directory**.

The screenshot shows a terminal window titled "Caesor@localhost:~/Documents". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output is as follows:

```
[Caesor@localhost Documents]$ ls
doc.tar.gz
[Caesor@localhost Documents]$ tar xvf doc.tar.gz
file1.txt
file2.txt
file3.txt
file4.txt
file5.txt
[Caesor@localhost Documents]$ ls
doc.tar.gz file1.txt file2.txt file3.txt file4.txt file5.txt
[Caesor@localhost Documents]$ ls
```

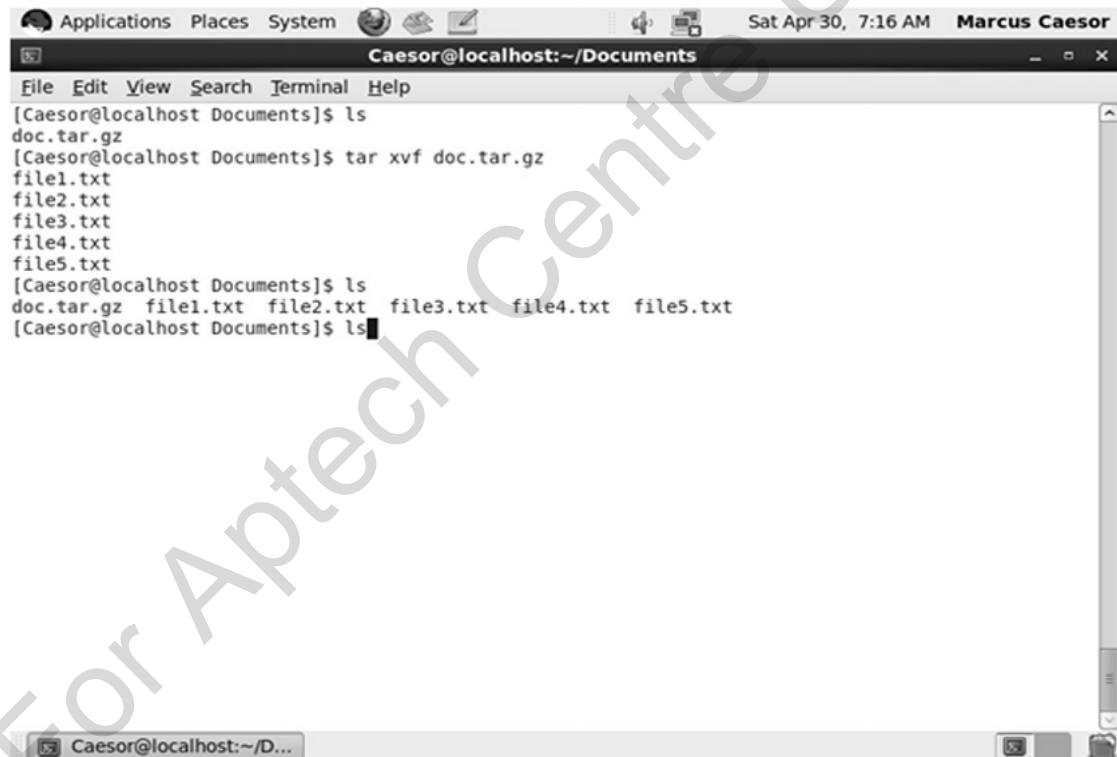
/etc/Directory

Exercise 1 [4-7]



Step 4

- Double-click auto.master to open the file.



```
Caesar@localhost:~/Documents
File Edit View Search Terminal Help
[Caesar@localhost Documents]$ ls
doc.tar.gz
[Caesar@localhost Documents]$ tar xvf doc.tar.gz
file1.txt
file2.txt
file3.txt
file4.txt
file5.txt
[Caesar@localhost Documents]$ ls
doc.tar.gz file1.txt file2.txt file3.txt file4.txt file5.txt
[Caesar@localhost Documents]$ ls
```

Contents of the auto.master File

Exercise 1 [5-7]



- In Step 4, study the contents of the file and notice there is a **/misc** directory mapping in this file.

Step 5

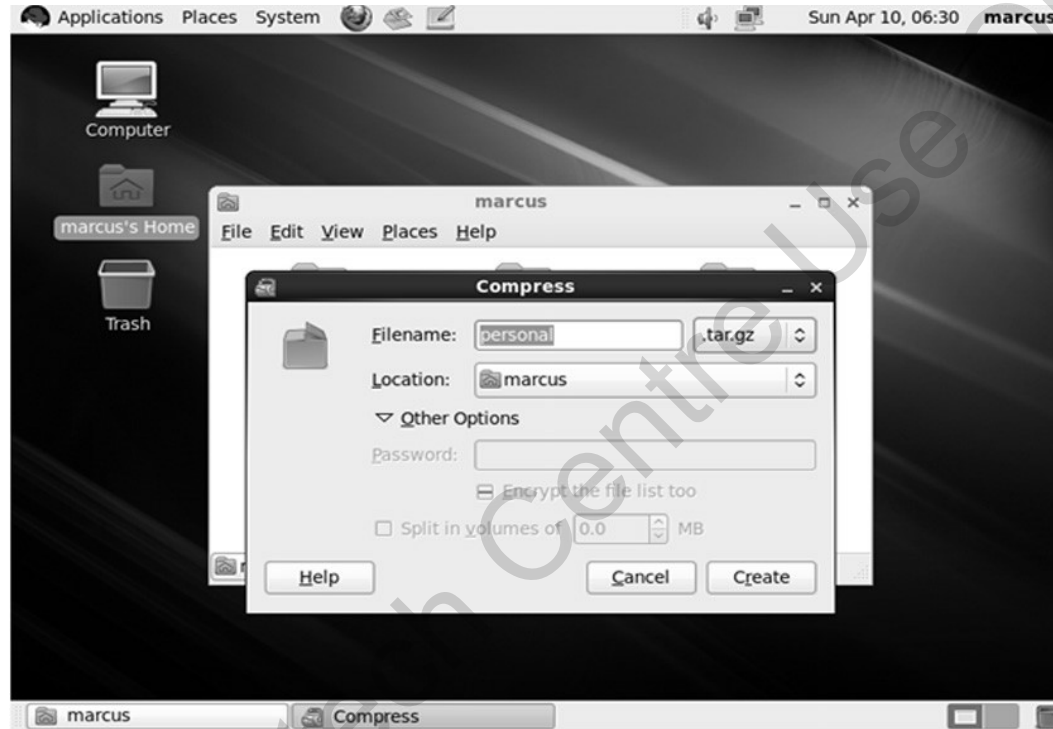
- Close the auto-master file.

Step 6

- In the **/etc/** directory, locate and open the **auto.misc** file.

Contents of the auto.master File

Exercise 1 [6-7]



Contents of the auto.misc File

- Notice that there is mapping of cd-rom marked with the following statement:

```
cd -fstype=iso9660, ro, nosuid, nodev :/dev/cdrom
```

Exercise 1 [7-7]



Step 7

- Review the file contents and close the file.

For Aptech Centre Use Only

Summary



- The three different methods of configuring network in RHEL are through the command line, through the graphical interface in X Window System and by configuring the configuration files.
- RHEL can be configured as a FTP server that can be configured to accept anonymous connections or to deny access to users. RHEL can also be configured as a Web server. By default, Apache is the Web server that can be configured on RHEL.
- There are different variants of Network File System (NFS). These are NFSv2, NFSv3, and NFSv4. NFSv4 communicates over TCP and uses port 2049. For NFS communication to take place, a client should mount the shares first. The mount command is used to mount the shares.
- NFS mount can be done using two methods. The first method is by using the /etc/fstab file and second method is the automount utility. The autofs service uses the automount daemon. It uses this daemon to monitor the preconfigured NFS mount points. The autofs service uses the /etc/auto.master file as the default configuration file.