I. File Systems

1. The ext3 File System

1.1. Features of ext3

Availability
Data Integrity
Speed
Easy Transition

1.2. Creating an ext3 File System

1. Create the partition using parted or fdisk.
2. Format the partition with the ext3 file system using mkfs.
3. Label the partition using e2label.
4. Create the mount point.
5. Add the partition to /etc/fstab.

1.3. Converting to an ext3 File System

#/sbin/tune2fs -j /dev/hdbX

To be certain to change the partition type from ext2 to ext3 in /etc/fstab.

Transitioning root file system - Use an initrd image (or RAM disk) to boot. To create this, run the mkinitrd program. Make sure your GRUB or LILO configuration loads the initrd.

1.4. Reverting to an ext2 File System

#umount /dev/hdbX
#/sbin/tune2fs -O ^has_journal /dev/hdb1
#/sbin/e2fsck -y /dev/hdb1
#mount -t ext2 /dev/hdb1 /mount/point
#rm -f .journal

2. Swap Space

2.1. What is Swap Space?

Swap space can be a dedicated swap partition (recommended), a swap file, or a combination of swap partitions and swap files.

The size of your swap space should be equal to twice your computer's RAM, or 32 MB, whichever amount is larger, but no more than 2048 MB (or 2 GB).

2.2. Adding Swap Space

To add a swap partition:

1. The hard drive can not be in use-skip the mount file system on booting OR unmount and turn off all the swap space on the hard drive with the swapoff command.
2. Create the swap partition using parted or fdisk:
   #parted /dev/hdb
   >(parted)#print
   >(parted)#mkpartfs part-type linux-swap start end
   >(parted)#quit
3. #mkswap /dev/hdb2
4. #swapon /dev/hdb2
5. Edit /etc/fstab
   /dev/hdb2 swap swap defaults 0 0
6. #cat /proc/swaps or #free

To add a swap file:

1. Determine the size of the new swap file and multiple by 1024 to determine the block size. For example, the block size of a 64 MB swap file is 65536.
2. #dd if=/dev/zero of=/swapfile bs=1024 count=65536
3. #mkswap /swapfile
4. #swapon /swapfile
5. Edit /etc/fstab to include:
   /swapfile swap swap defaults 0 0
6. #cat /proc/swaps or #free

2.3. Removing Swap Space

To remove a swap partition:

1. The hard drive can not be in use-skip the mount file system on booting OR unmount and turn off all the swap space on the hard drive with the swapoff command.

2. #swapoff /dev/hdb2

3. Remove its entry from /etc/fstab

4. Remove the partition using parted or fdisk:

```
#parted /dev/hdb
>(parted)#print
>(parted)#r m MINOR          ;MINOR is the minor number of the partition
>(parted)#quit
```

To remove a swap file:

1. #swapoff /swapfile
2. Remove its entry from /etc/fstab.
3. #rm /swapfile

2.4. Moving Swap Space

To move swap space from one location to another, follow the steps for removing swap space, and then follow the steps for adding swap space.

3. Redundant Array of Independent Disks (RAID)

3.1. What is RAID?

RAID is a method in which information is spread across several disks, using techniques such as disk striping (RAID Level 0), disk mirroring (RAID level 1), and disk striping with parity (RAID Level 5) to achieve redundancy, lower latency and/or increase bandwidth for reading or writing to disks, and maximize the ability to recover from hard disk crashes.

3.2. Who Should Use RAID?

- Enhanced speed
- Increased storage capacity using a single virtual disk
- Lessened impact of a disk failure

3.3. Hardware RAID versus Software RAID

Software RAID offers:

- Threaded rebuild process
- Kernel-based configuration
- Portability of arrays between Linux machines without reconstruction
- Backgrounded array reconstruction using idle system resources
- Hot-swappable drive support
- Automatic CPU detection to take advantage of certain CPU optimizations

**A hot-swap chassis allows you to remove a hard drive without having to power-down your system.*

3.4. RAID Levels and Linear Support

1. *Level 0* — RAID level 0, often called "striping," is a performance-oriented striped data mapping technique. The storage capacity of a level 0 array is equal to the total capacity of the member disks in a Hardware RAID or the total capacity of member partitions in a Software RAID.

2. *Level 1* — RAID level 1, or "mirroring," has been used longer than any other form of RAID. Level 1 provides redundancy by writing identical data to each member disk of the array, leaving a "mirrored" copy on each disk.

3. *Level 4* — Level 4 uses parity [2] concentrated on a single disk drive to protect data. It is better suited to transaction I/O rather than large file transfers. Because the dedicated parity disk represents an inherent bottleneck, level 4 is seldom used without accompanying technologies such as write-back caching.

4. *Level 5* — This is the most common type of RAID. By distributing parity across some or all of an array's member disk drives, RAID level 5 eliminates the write bottleneck inherent in level 4. The only performance bottleneck is the parity calculation process. With modern CPUs and Software RAID, that usually is not a very big problem.

5. *Linear RAID* — Linear RAID is a simple grouping of drives to create a larger virtual drive. In linear RAID, the chunks are allocated sequentially from one member drive, going to the next drive only when the first is completely filled.

** RAID level 4 takes up the same amount of space as RAID level 5, but level 5 has more advantages. For this reason, level 4 is not supported.*

4. Logical Volume Manager (LVM)

LVM is a method of allocating hard drive space into logical volumes that can be easily resized instead of partitions.

With LVM, the hard drive or set of hard drives is allocated to one or more physical volumes. A physical volume can not span over more than one drive.

LVM support must be compiled into the kernel. The default kernel for Red Hat Linux 9 is compiled with LVM support.

5. Managing Disk Storage

parted commands

check minor-num	Perform a simple check of the file system
cp from to	Copy file system from one partition to another; from and to are the minor numbers of the partitions
help	Display list of available commands
mklabel label	Create a disk label for the partition table
mkfs minor-num file-system-type	Create a file system of type file-system-type
mkpart part-type fs-type start-mb end-mb	Make a partition without creating a new file system
mkpartfs part-type fs-type start-mb end-mb	Make a partition and create the specified file system
move minor-num start-mb end-mb	Move the partition
print	Display the partition table
quit	Quit parted
resize minor-num start-mb end-mb	Resize the partition from start-mb to end-mb
rm minor-num	Remove the partition
select device	Select a different device to configure
set minor-num flag state	Set the flag on a partition; state is either on or off

5.1. Viewing the Partition Table

```
>(parted)#print
```

5.2. Creating a Partition

```
#parted /dev/hda
>(parted)#print
```

Making the Partition

```
>(parted)#mkpart primary ext3 1024 2048
#cat /proc/partitions
```

Formating the Partition

```
#/sbin/mkfs -t ext3 /dev/hdb3
```

Labeling the Partition

```
#e2label /dev/hda3 /work
```

Creating the Mount Point

```
#mkdir /work
```

Add to /etc/fstab

```
LABEL=/work     /work           ext3    defaults        1 2
#mount /work                    ;without rebooting
```

5.3. Removing a Partition

```
#parted /dev/hda
>(parted)#print
>(parted)#rm 3                  ;3 = minor number
#cat /proc/partitions
Remove its line from the /etc/fstab file
```

5.4. Resizing a Partition

```
#parted /dev/hda
>(parted)#print
>(parted)#resize 3 1024 2048
```

** The used space of the partition to resize must not be larger than the new size.*

6. Implementing Disk Quotas

6.1. Configuring Disk Quotas

1. Enable quotas per file system by modifying /etc/fstab

```
LABEL=/          /                       ext3    defaults              1 1
LABEL=/boot      /boot                   ext3    defaults              1 2
none             /dev/pts                devpts  gid=5,mode=620              0 0
LABEL=/home              /home                   ext3    defaults,usrquota,grpquota 1 2
none             /proc           proc    defaults        0 0
none             /dev/shm        tmpfs   defaults        0 0
/dev/hda2        swap            swap    defaults        0 0
/dev/cdrom       /mnt/cdrom      udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0         /mnt/floppy     auto    noauto,owner,kudzu          0 0
```

2. Remount the file system(s)

#umount and #mount

3. Create the quota files and generate the disk usage table

The quotacheck command examines quota-enabled file systems and builds a table of the current disk usage per file system.

#quotacheck -acug /home OR

#quotacheck -avug

a — Check all quota-enabled, locally-mounted file systems

v — Display verbose status information as the quota check proceeds

u — Check user disk quota information

g — Check group disk quota information

4. Assign quotas

#edquota username

Disk quotas for user testuser (uid 501):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/hda3	440436	0	0	37418	0	0

#quota testuser

5. Assigning Quotas per Group

#edquota -g devel

Disk quotas for group devel (gid 505):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/hda3	440400	0	0	37418	0	0

#quota -g devel

6. Assigning Quotas per File System

#edquota -t

Grace period before enforcing soft limits for users:

Time units may be: days, hours, minutes, or seconds

Filesystem	Block grace period	Inode grace period
/dev/hda3	7days	7days

6.2. Managing Disk Quotas

1. <u>Reporting on Disk Quotas</u>

#repquota /home

*** Report for user quotas on device /dev/hda3

Block grace time: 7days; Inode grace time: 7days

		Block limits				File limits			
User	used		soft	hard	grace	used	soft	hard	grace
root	--	36	0	0		4	0	0	
tfox	--	540	0	0		125	0	0	
testuser	–	440400	500000	550000		37418	0	0	

* "–" is the quota exceeded? Block (-) and INODE (-) [+,-]

** "grace" records equal to the amount of time remaining on the grace period

#repquota -a

2. <u>Keeping Quotas Accurate</u>

#quotacheck -avug

To run it periodically is to use cron

/etc/cron.hourly

/etc/cron.daily

/etc/cron.weekly

/etc/cron.monthly

3. Enabling and Disabling

#quotaoff -vaug
#quotaon -vaug ;OR
#quotaon -vug /home ;for a specific file system

6.3. Additional Resources

Installed Documentation

The quotacheck, edquota, repquota, quota, quotaon, and quotaoff man pages

II. Installation-Related Information

7. Kickstart Installations

7.1. What are Kickstart Installations?

Kickstart lets you automate a Red Hat Linux installation. Using kickstart, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical Red Hat Linux installation.

7.2. How Do You Perform a Kickstart Installation?

1. Create a kickstart file.
2. Create a boot diskette with the kickstart file or make the kickstart file available on the network.
3. Make the installation tree available.
4. Start the kickstart installation.

7.3. Creating the Kickstart File

- The kickstart file is a simple text file, containing a list of items, each identified by a keyword.
- Sample.ks file found in the RH-DOCS directory of the Red Hat Linux Documentation CD.
- The options selected during installation are written to the file /root/anaconda-ks.cfg.
- Sections must be specified in order. Items within the sections do not have to be in a specific order unless otherwise specified.
- Items that are not required can be omitted.
- Omitting any required item will result in the installation progr am prompting the user for an answer to the related item.
- Lines starting with a pound sign (#) are treated as comments and are ignored.
- For kickstart upgrades, the following items are required:
  - Language
  - Language support
  - Installation method
  - Device specification (if device is needed to perform installation)
  - Keyboard setup
  - The upgrade keyword
  - Boot loader configuration

7.4. Kickstart Options

7.5. Package Selection

7.6. Pre-installation Script

7.7. Post-installation Script

7.8. Making the Kickstart File Available

1. The kickstart file must be named ks.cfg and must be located in the boot diskette's top-level directory.

2. Because the Red Hat Linux boot diskettes are in MS-DOS format, it is easy to copy the kickstart file under Linux using the mcopy command:

C:\>mcopy ks.cfg a: ; OR
#cp ;for linux

3. If a kickstart file is specified by the BOOTP/DHCP server, the client system will attempt an NFS mount of the file's path, and will copy the specified file to the client, using it as the kickstart file. The exact settings required vary depending on the BOOTP/DHCP server you use.

!DHCP Server Script
filename "/usr/new -machine/kickstart/";

next-server blarg.redhat.com;

4. Note that you should replace the value after filename with the name of the kickstart file (or the directory in which the kickstart file resides) and the value after next-server with the NFS server name.

5. If the filename returned by the BOOTP/DHCP server ends with a slash ("/"), then it is interpreted as a path only. In this case, the client system mounts that path using NFS, and searches for a particular file. The filename the client searches for is:

<ip-addr>-kickstart

** The <ip-addr> section of the filename should be replaced with the client's IP address in dotted decimal notation. For example, the filename for a computer with an IP address of 10.10.0.1 would be 10.10.0.1-kickstart.*

6. If you do not specify a server name, then the client system will attempt to use the server that answered the BOOTP/DHCP request as its NFS server. If you do not specify a path or filename, the client system will try to mount /kickstart from the BOOTP/DHCP server and will try to find the kickstart file using the same <ip-addr>-kickstart filename as described above.

7.9. Making the Installation Tree Available

7.10. Starting a Kickstart Installation

Boot Diskette

linux ks=floppy

CD-ROM #1 and Diskette

linux ks=floppy ; OR

linux ks=hd:fd0:/ks.cfg

With Driver Disk

linux ks=floppy dd

Boot CD-ROM

linux ks=cdrom:/ks.cfg

Other options to start a kickstart installation are as follows:

ks=nfs:<server>:/<path>
ks=http://<server>/<path>
ks=floppy
ks=floppy:/<path>
ks=hd:<device>:/<file>
ks=hd:sda3:/mydir/ks.cfg
ks=file:/<file>
ks=cdrom:/<path>
ksdevice=<device>
ks

If DHCP is specified and the bootfile begins with a /, the bootfile provided by DHCP is looked for on the NFS server.

If DHCP is specified and the bootfile begins with something other then a /, the bootfile provided by DHCP is looked for in the /kickstart directory on the NFS server.

If DHCP did not specify a bootfile, then the installation program tries to read the file /kickstart/1.2.3.4-kickstart, where 1.2.3.4 is the numeric IP address of the machine being installed.

8. Kickstart Configurator

9. Basic System Recovery

9.1. Common Problems

1. Unable to Boot into Red Hat Linux (runlevel 3 or 5)
   - Caused by the installation of another operating system after you have installed Red Hat Linux. They overwrite the Master Boot Record (MBR) that originally contained the GRUB or LILO boot loader.
     Solution: Get into rescue mode and reconfigure the boot loader.
   - Changes the order of your partitions by using a partitioning tool to resize a partition or create a new partition from free space after installation.
     Solution: boot in rescue mode and modify /boot/grub/grub.conf if you are using GRUB or /etc/lilo.conf if you are using LILO. You must also run the /sbin/lilo command anytime you modify the LILO configuration file.

2. Hardware/Software Problems
   Solution: Boot into one of the system recovery modes, you might be able to resolve the problem or at least get copies of your most important files.

3. Root Password
   Solution: To reset it to a different password, boot into RESCUE mode or SINGLE-USER mode and use the passwd command to reset the root password.

9.2. Booting into Rescue Mode

1. To boot into rescue mode:
   - By booting the system from an installation boot diskette made from the bootdisk.img image.
     * To create an installation boot diskette, insert a blank diskette and use the images/bootdisk.img file on the Red Hat Linux CD-ROM #1 with the command dd if=bootdisk.img of=/dev/fd0.
   - By booting the system from an installation boot CD-ROM.
   - By booting the system from the Red Hat Linux CD-ROM #1.
2. >(PROMPT)# linux rescue
3. -/bin/sh-2.05b#
4. #chroot /mnt/sysimage
5. #mount -t ext3 /dev/hda5 /foo
6. #fdisk -l

9.3. Booting into Single-User Mode (runlevel 1)

- Unlike rescue mode, single-user mode automatically tries to mount your file system.
- GRUB
  1. If you have a GRUB password configured, type p and enter the password.
  2. Select Red Hat Linux with the version of the kernel that you wish to boot and type e for edit. You will be presented with a list of items in the configuration file for the title you have selected.
  3. Select the line that starts with kernel and type e to edit the line.
  4. Go to the end of the line and type single as a separate word (press the [Spacebar] and then type single). Press [Enter] to exit edit mode.
  5. Back at the GRUB screen, type b to boot into single-user mode.
- LILO
  1. If you are using the graphical LILO, you must press [Ctrl]-[x] to exit the graphical screen and go to the boot: prompt.
  2. linux single

9.4. Booting into Emergency Mode

To boot into emergency mode, use the same method as described for single-user mode with one exception, replace the keyword single with the keyword emergency.

10. Software RAID Configuration

11. LVM Configuration

III. Network-Related Configuration

12. Network Configuration

#redhat-config-network

The Network Administration Tool can be used to configure the following types of network interfaces:

- Ethernet
- ISDN
- modem
- xDSL
- token ring
- CIPE
- wireless devices

12.1. Overview

1. Add the physical hardware device to the hardware list.
2. Add a network device associated with the physical hardware device.
3. Configure the hostname and DNS settings.
4. Configure any hosts that cannot be looked up through DNS.

12.2. Establishing an Ethernet Connection

A device alias allows you to setup multiple virtual devices for one physical device, thus giving the one physical device more than one IP address. For example, you can configure an eth1 device and an eth1:1 device.

** Be sure to select File => Save to save the changes*

12.3. Establishing an ISDN Connection
12.4. Establishing a Modem Connection
12.5. Establishing an xDSL Connection
12.6. Establishing a Token Ring Connection
12.7. Establishing a CIPE Connection
12.8. Establishing a Wireless Connection
12.9. Managing DNS Settings

12.10. Managing Hosts

#cat /etc/hosts

#cat /etc/host.conf

To change lookup order, edit the /etc/host.conf file. The line order hosts, bind specifies that the /etc/hosts takes precedence over the name servers. Changing the line to order bind, hosts configures the system to resolve hostnames and IP addresses using the name servers first. If the IP address cannot be resolved through the name servers, the system then looks for the IP address in the /etc/hosts file.

12.11. Activating Devices

#redhat-control-network

12.12. Working with Profiles

- Logical networkdevices are different from device aliases: They cannot be activated simultaneously.
- Profiles can be used to create multiple configuration sets for different networks.
- A configuration set can include logical devices as well as hosts and DNS settings.
- After configuring the profiles, you can use the Network Administration Tool to switch back and forth between them.
- STEPS:
    1. Click on an existing device already in the list,
    2. Click the Copy button to copy the existing device to a logical network device. (If you use the New button, a network alias will be created, which is incorrect.)
    3. To change the properties of the logical device, select it from the list and click Edit.
- #redhat-control-network
- #redhat-config-network-cmd --profile <profilename> --activate

12.13. Device Aliases

- Can be activated at the same time to have different IP addresses.
- Be represented as the device name followed by a colon and a number (for example, eth0:1).
- Use a static IP address (DHCP does not work with aliases)
- STEPS:
    1. #redhat-control-network
    2. Devices tab and click New
    3. Select the Ethernet card to configure with an alias
    4. Set the static IP address for the alias
    5. Click Apply to create it

#/sbin/ifconfig ; Check it

13. Basic Firewall Configuration

13.1. Security Level Configuration Tool

High:

By default, only the following connections are allowed:

- DNS replies
- DHCP — so any network interfaces that use DHCP can be properly configured

Not allow the following:

- Active mode FTP (passive mode FTP, used by default in most clients, should still work)
- IRC DCC file transfers
- RealAudio
- Remote X Window System clients

Medium:

Not allowed:

- Ports lower than 1023 — the standard reserved ports, used by most system services, such as FTP, SSH, telnet, HTTP, and NIS.
- The NFS server port (2049) — NFS is disabled for both remote severs and local clients.
- The local X Window System display for remote X clients.
- The X Font server port (by default, xfs does not listen on the network; it is disabled in the font server).

** Select a medium or high firewall, network authentication methods (NIS and LDAP) will not work*

- Use iptables commands
- Written to the /etc/sysconf ig/iptables
- The options selected are also written to /etc/sysconfig/redhat-config-securitylevel

13.2. GNOME Lokkit

GNOME Lokkit allows you to configure firewall settings for an average user by constructing basic iptables networking rules. Instead of having to write the rules, this program asks you a series of questions about how you use your system and then writes it for you in the file /etc/sysconfig/iptables.

13.3. Activating the iptables Service

```
#/sbin/service iptables restart                 ;Restart the services
#/sbin/chkconfig --level 345 iptables on        ;Turn On
#/sbin/chkconfig --level 345 ipchains off       ;Turn Off
```

14. Controlling Access to Services

Both the services managed by xinetd (discussed later in this section) and the services in the /etc/rc.d hierarchy can be configured to start or stop using three different applications:

1. Services Configuration Tool
2. ntsysv
3. chkconfig

Related files: /etc/rc.d AND /etc/xinetd.d

14.1. Runlevels

0 — Halt
1 — Single-user mode
2 — Not used (user-definable)
3 — Full multi-user mode
4 — Not used (user-definable)
5 — Full multi-user mode (with an X-based login screen)
6 — Reboot

- The services listed in the directory /etc/rc.d/rc<x>.d, where <x> is the number of the runlevel.
- If you use a text login screen, you are operating in runlevel 3. If you use a graphical login screen, you are operating in runlevel 5.
- The default runlevel can be changed by modifying the /etc/inittab file, which contains a line near the top of the file similar to the following:

```
#cat /etc/inittab
id:5:initdefault:
```

- To change the runlevel immediately, use the command telinit

```
#telinit <level_number>
```

14.2. TCP Wrappers

- xinetd can use the /etc/hosts.allow and /etc/hosts.deny files to configure access to system services.
- The hosts.allow file takes precedence over the hosts.deny file.
- #man 5 hosts_access ;Document

- To control access to Internet services, use xinetd, which is a secure replacement for inetd.
- The configuration file for xinetd is /etc/xinetd.conf
    #cat /etc/xinetd.conf
- Include the /etc/xinetd.d directory
    -/etc/xinetd.d/
    -Edit configuration file in the /etc/xinetd.d directory.
        -If the disable attribute is set to yes, the service is disabled. If the disable attribute is set to no, the service is enabled.
- #/etc/xinetd.d. ; Review the contents of the /etc/xinetd.d directory

14.3. Services Configuration Tool

The Services Configuration Tool lists the services from the /etc/rc.d/init.d directory as well as the services controlled by xinetd.

14.4. ntsysv

#ntsysv ;The current runlevel
#ntsysv --level 345 ;Specity configuration for runlevel 345
- The [F1] key will pop up a short description of each service
- Services managed by xinetd are immediately affected by ntsysv.
- For all other services, changes do not take effect immediately.
- You must stop or start the individual service with the command service daemon stop.
    #service <daemon> <[stop,start,restart]>

14.5. chkconfig

#chkconfig --list
- Query a service in /etc/rc.d
- See a list of system services and whether they are started (on) or stopped (off) in runlevels 0-6.
- At the end of the list, you will see a section for the services managed by xinetd.

#chkconfig --level 345 <daemon> off

14.6. Additional Resources
- The man pages for ntsysv, chkconfig, xinetd, and xinetd.conf
- man 5 hosts_access

15. OpenSSH

OpenSSH is a free, open source implementation of the SSH (Secure SHell) protocols. It replaces telnet, ftp, rlogin, rsh, and rcp with secure, encrypted network connectivity tools.

15.1. Why Use OpenSSH?

1. Enhancing the security
2. Automatically forwards the DISPLAY variable to the client machine

15.2. Configuring an OpenSSH Server
- openssh-server package is required and depends on the openssh package.
- /etc/ssh/sshd_config ;Configuration file
- #man sshd
- #/sbin/service sshd <start,stop>
- Keep the host keys generated for the system,
    1. Backup the /etc/ssh/ssh_host*key* files
    2. Restore them after the reinstall.

15.3. Configuring an OpenSSH Client

1. Using the ssh Command
    - openssh-clients AND openssh packages installed
    - #ssh penguin.example.net
    - ssh -l <username> penguin.example.net ;Specify a different username
    - ssh penguin.example.net ls /usr/share/doc ;Used to execute a command on the remote machine without logging in to a shell prompt

2. Using the scp Command
    - The scp command can be used to transfer files between machines over a secure, encrypted connection. It is similar to rcp.
    - #scp localfile username@tohostname:/newfilename ; ;Upload
    - #scp shadowman username@penguin.example.net:/home/username ;eg. Upload
    - #scp username@tohostname:/remotefile /newlocalfile ;Download

- #scp /downloads/* username@penguin.example.net:/uploads/ ;Multiple files

3. Using the sftp Command
- #sftp username@hostname.com.
- #man sftp
* The sftp utility is only available in OpenSSH version 2.5.0p1 and higher

4. Generating Key Pairs
- Do not have to enter your passw ord every time you use ssh, scp, or sftp to connect to a remote machine.
- Starting with OpenSSH version 3.0, ~/.ssh/authorized_keys2, ~/.ssh/known_hosts2, and /etc/ssh_known_hosts2 are obsolete. SSH Protocol 1 and 2 share the ~/.ssh/authorized_keys, ~/.ssh/known_hosts, and /etc/ssh/ssh_known_hosts files.
- Backup the .ssh directory in your home directory. After reinstalling, copy this directory back to your home directory.
* Red Hat Linux 9 uses SSH Protocol 2 and RSA keys by default.
STEPS:
1. Generating an RSA Key Pair for Version 2
#ssh-keygen -t rsa ;The public key is written to ~/.ssh/id_rsa.pub. The private key is written to ~/.ssh/id_rsa.
#chmod 755 ~/.ssh.
-Copy the contents of ~/.ssh/id_rsa.pub to ~/.ssh/authorized_keys on the machine to which you want to connect.
*If the file ~/.ssh/authorized_keys does not exist, you can copy the file ~/.ssh/id_rsa.pub to the file ~/.ssh/authorized_keys on the other machine.
2. Configuring ssh-agent
GNOME
- #rpm -q openssh-askpass-gnome
- Select Main Menu Button (on the Panel) => Preferences => More Preferences => Sessions, and click on the Startup Programs tab. Click Add and enter /usr/bin/ssh-add in the Startup Command text area. Set it a priority to a number higher than any existing commands to ensure that it is executed last. A good priority number for ssh-add is 70 or higher. The higher the priority number, the lower the priority. If you have other programs listed, this one should have the lowest priority. Click Close to exit the program.
- Log out and then log back into GNOME; in other words, restart X. After GNOME is started, a dialog box will appear prompting you for your passphrase(s). Enter the passphrase requested. If you have both DSA and RSA key pairs configured, you will be prompted for both. From this point on, you should not be prompted for a password by ssh, scp, or sftp.
X Window
- #exec /usr/bin/ssh-agent $SHELL
- #ssh-add
- When you log out, your passphrase(s) will be forgotten. You must execute these two commands each time you log in to a virtual console or open a terminal window.

15.4. Additional Resources

The ssh, scp, sftp, sshd, and ssh-keygen man pages

16. Network File System (NFS)

16.1. Why Use NFS?

16.2. Mounting NFS File Systems

#mount shadowman.example.com:/misc/export /misc/local

Mounting NFS File Systems using /etc/fstab

server:/usr/local/pub /pub nfs rsize=8192,wsize=8192,timeo=14,intr

#mount /pub

Mounting NFS File Systems using autofs

- /etc/auto.master ;Autofs consults the master map configuration file /etc/auto.master to determine which mount points are defined.
- #cat /etc/auto.master
/misc /etc/auto.misc --timeout 60
* The first field is the mount point. The directory /misc must exist on the local file system.
* The second field is the location of the map file.
* The third field is optional. The third field can contain information such as a timeout value.
- #cat /etc/auto.misc
myproject -rw,soft,intr,rsize=8192,wsize=8192 penguin.example.net:/proj52
* The first field in /etc/auto.misc is the name of the /misc subdirectory; No need to create.
* The second field contains mount options such as rw for read and write access.

* The third field is the location of the NFS export including the hostname and directory.
- #/sbin/service autofs restart
- #/sbin/service autofs status
- #/sbin/service autofs reload ;Modify the /etc/auto.master and Reload

16.3. Exporting NFS File Systems

#cat /etc/exports
;directory hostname(options)
;options are *sync or async //If sync is specified, the server does not reply to requests before the changes made by the request are written to the disk.
;default is read-only
/misc/export speedy.example.com(sync)
/misc/export speedy.example.com(rw,sync)
!!!Be careful with spaces in the /etc/exports file. No space between the hostname and the options.
#/sbin/service nfs reload ;If modify /etc/exports
Hostname Formats
- Single machine — A fully qualified domain name (that can be resolved by the server), hostname (that can be resolved by the server), or an IP address.
- Series of machines specified with wildscards — Use the * or ? character to specify a string match. (*.example.com = one.example.com <> one.two.example.com)
- IP networks — Use a.b.c.d/z, where a.b.c.d is the network and z is the number of bits in the netmask (192.168.0.0/24 OR 192.168.100.8/255.255.255.0)
- Netgroups — In the format @group-name, where group-name is the NIS netgroup name.
#/sbin/service nfs <status,start,stop>
#/sbin/chkconfig --level 345 nfs on

16.4. Additional Resources

The man pages for nfsd, mountd, exports, auto.master, and autofs (in manual sections 5 and 8)

17. Samba

17.1. Why Use Samba?

17.2. Configuring a Samba Server

- #cat /etc/samba/smb.conf
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
- #/sbin/service smb restart ;If modify /etc/exports

Encrypted Passwords
#cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd ;For Local OR
#ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd ;For NIS
#chmod 600 /etc/samba/smbpasswd
* The mksmbpasswd.sh script is installed in your /usr/bin directory with the samba package.
#smbpasswd username ;For each username-Default account will not activate-Use the password should be used different from linux.
#cat /etc/samba/smb.conf
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd
#service smb restart
** Read /usr/share/doc/samba-<version>/docs/htmldocs/ENCRYPTION.html to learn more about encrypted passwords. (replace <version> with the version number of Samba that you have installed).*

The pam_smbpass PAM module can be used to sync users' Samba passwords with their system passwords when the passwd command is used. If a user invokes the passwd command, the password he uses to log in to the Red Hat Linux system as well as the password he must provide to connect to a Samba share are changed.

To enable this feature, add the following line to /etc/pam.d/system-auth below the pam_cracklib.so invocation:

#cat /etc/pam.d/system-auth
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass

Starting and Stopping the Server
#/sbin/service smb <status,start,stop>
#/sbin/chkconfig --level 345 smb on

17.3. Connecting to a Samba Share

Windows Client
Use Network Neighborhood or the graphical file manager.
Linux Client
#smbclient //hostname/sharename -U username
smb:\> exit ;OR
- Type smb: in the location bar of Nautilus to view the workgroups. OR
- Type smb://user:password@servername/sharename/

17.4. Additional Resources

smb.conf man page — explains how to configure the Samba configuration file
smbd man page — describes how the Samba daemon works
/usr/share/doc/samba-<version-number>/docs/ — HTML and text help files included with the samba package

18. Dynamic Host Configuration Protocol (DHCP)

18.1. Why Use DHCP?

18.2. Configuring a DHCP Server

!#cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf

#cat /etc/dhcpd.conf

```
ddns-update-style interim;
#ddns-update-style ad-hoc;
#Subnet Declaration
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask                      255.255.255.0;
        option domain-name                      "example.com";
        option domain-name-servers              192.168.1.1;
        option time-offset              -18000;     # Eastern Standard Time
        range 192.168.1.10 192.168.1.100;
}
#Shared-network Declaration
shared-netw ork name {
        option domain-name                      "test.redhat.com";
        option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
        option routers                  192.168.1.254;
        #more parameters for EXAMPLE shared-network
        subnet 192.168.1.0 netmask 255.255.255.0 {
                #parameters for subnet
                range 192.168.1.1 192.168.1.31;
        }
        subnet 192.168.1.32 netmask 255.255.255.0 {
                #parameters for subnet
                range 192.168.1.33 192.168.1.63;
        }
}
#Group Declaration
group {
        option routers                  192.168.1.254;
        option subnet-mask                      255.255.255.0;
        option domain-name                      "example.com";
        option domain-name-servers              192.168.1.1;
        option time-offset              -18000;     # Eastern Standard Time
        host apex {
```

```
                option host-name "apex.example.com";
                hardware ethernet 00:A0:78:8E:9E:AA;
                fixed-address 192.168.1.4;
        }

        host raleigh {
                option host-name "raleigh.example.com";
                hardware ethernet 00:A1:DD:74:C3:F2;
                fixed-address 192.168.1.6;
        }
}
#Range Parameter
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.10 192.168.1.100;
}
#Static IP Address using DHCP
host apex {
        option host-name "apex.example.com";
        hardware ethernet 00:A0:78:8E:9E:AA;
        fixed-address 192.168.1.4;
}
#-----------------------------------------------------------------------------------#
```

/var/lib/dhcp/dhcpd.leases

#service dhcpd restart ;If modify the configuration file

** The keywords are case-insensitive, and lines beginning with a hash mark (#) are considered comments.*

#cat /etc/sysconfig/dhcpd

```
# Command line options here
# Service only eth0
DHCPDARGS=eth0
```

** The default is port 67. The DHCP server transmits responses to the DHCP clients at a port number one greater than the udp port specified. For example, if you accept the default of port 67, the server listens on port 67 for requests and responses to the client on port 68.*

DHCP Relay Agent

- Relay DHCP and BOOTP requests from a subnet to one or more DHCP servers on other subnets.
- The DHCP Relay Agent forwards the request to the list of DHCP servers specified when the DHCP Relay Agent is started.
- /etc/sysconfig/dhcrelay => with the INTERFACES directive.
- #service dhcrelay start ;To start the DHCP Relay Agent

18.3. Configuring a DHCP Client

#cat /etc/sysconfig/network

```
NETWORKING=yes
```

#cat /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

18.4. Additional Resources

dhcpd man page — describes how the DHCP daemon works

dhcpd.conf man page — explains how to configure the DHCP configuration file; includes some examples

dhcpd.leases man page — explains how to configure the DHCP leases file; includes some examples

dhcp-options man page — explains the syntax for declaring DHCP options in dhcpd.conf; includes some examples

dhcrelay man page — explains the DHCP Relay Agent and its configuration options.

19. Apache HTTP Server Configuration

- /etc/httpd/conf/httpd.conf
- It does not use the old srm.conf or access.conf configuration files; leave them empty
- The httpd and redhat-config-httpd RPM packages need to be installed to use the HTTP Configuration Tool.
- #redhat-config-httpd

19.1. Basic Settings

#cat /etc/httpd/conf/httpd.conf

ServerName www.domain.com
ServerAdmin root@localhost
Listen 80

19.2. Default Settings

#cat /etc/httpd/conf/httpd.conf

DirectoryIndex index.html, index.htm, index.shtml
ErrorDocument /var/www/html/errors/404.html
TransferLog ;/var/log/httpd/access_log, /var/log/httpd/error_log
LogFormat
ErrorLog
LogLevel
HostnameLookups ;<Reverse Lookup,Double Reverse Lookup, *No Reverse Lookup>
#The Apache HTTP Server can use the mod_env module to configure the environment variables which are passed to CGI scripts and SSI pages.
SetEnv
PassEnv
UnsetEnv
<Directory>
Order
#If you check the Let .htaccess files override directory options, the configuration directives in the .htaccess file take precedence.

19.3. Virtual Hosts Settings

#cat /etc/httpd/conf/httpd.conf

<VirtualHost> {
DocumentRoot ;/var/www/html
ServerAdmin
}
#Host Information ;<Default Virtual Host, IP based Virtual Host, Name based Virtual Host>
<NameVirtualHost>
ServerAlias

Apache SSL:

- Enabling Apache SSL support enables the use of the mod_ssl security module.
- Allow access through port 443

19.4. Server Settings

#cat /etc/httpd/conf/httpd.conf

LogFile
PidFile
CoreDumpDirectory ; The default value is the ServerRoot
User ; The default for User is apache.
Group ; The default for User is apache.

19.5. Performance Tuning

#cat /etc/httpd/conf/httpd.conf

MaxClients 150 ; Can not set this value to higher than 256 without recompiling.
TimeOut 300 ; Second
MaxRequestsPerChild 100
MaxKeepAliveRequests 0 ; Allow unlimited requests per connection - 0 = unlimited
KeepAlive
KeepAliveTimeout

19.6. Saving Your Settings

Saved in /etc/httpd/conf/httpd.conf

/etc/httpd/conf/httpd.conf => /etc/httpd/conf/httpd.conf.bak.
#service httpd restart

19.7. Additional Resources
/usr/share/docs/httpd-<version>

20. Apache HTTP Secure Server Configuration

20.1. Introduction
/etc/httpd/conf.d/ssl.conf
#cat /etc/httpd/conf/httpd.conf
Include conf.d/*.conf
* The mod_ssl configuration file is located at /etc/httpd/conf.d/ssl.conf. For this file to be loaded, and hence for mod_ssl to work, you must have the statement Include conf.d/*.conf in /etc/httpd/conf/httpd.conf. This statement is included by default in the default Apache HTTP Server configuration file in Red Hat Linux 9.

20.2. An Overview of Security-Related Packages
20.3. An Overview of Certificates and Security
20.4. Using Pre-Existing Keys and Certificates
20.5. Types of Certificates
20.6. Generating a Key
20.7. Generating a Certificate Request to Send to a CA
20.8. Creating a Self-Signed Certificate
20.9. Testing The Certificate
20.10. Accessing The Server
20.11. Additional Resources

21. BIND Configuration
#redhat-config-bind

21.1. Adding a Forward Master Zone
#cat /etc/named.conf
```
zone  "forward.example.com" {
        type master ;
        file  "forward.example.com.zone";
};
```
#ls -la /var/named
#cat /var/named/forward.example.com.zone
```
$TTL 86400
@       IN      SOA     ns.example.com.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )

        IN      NS      192.168.1.1.
```

21.2. Adding a Reverse Master Zone
#cat /etc/named.conf
```
zone  "10.168.192.in-addr.arpa" {
        type master;
        file  "10.168.192.in-addr.arpa.zone";
};
```
#cat /var/named/10.168.192.in-addr.arpa.zone
```
$TTL 86400
@       IN      SOA     ns.example.com. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
                        )
@       IN      NS      ns2.example.com.
```

```
1       IN      PTR     one.example.com.
2       IN      PTR     tw o.example.com.
```

21.3. Adding a Slave Zone

```
#cat /etc/named.conf
        zone "slave.example.com" {
                type slave;
                file "slave.example.com.zone";
                masters {
                                1.2.3.4;
                        };
        };
```

** The configuration file /var/named/slave.example.com.zone is created by the named service when it downloads the zone data from the master server(s).*

22. Authentication Configuration

22.1. User Information

- Cache User Information — Select this option to enable the name service cache daemon (nscd) and configure it to start at boot time.

*The nscd package must be installed for this option to work.

- Enable NIS Support — Select this option to configure the system as an NIS client which connects to an NIS server for user and password authentication. Click the Configure NIS button to specify the NIS domain and NIS server. If the NIS server is not specified, the daemon will attempt to find it via broadcast.

*The ypbind package must be installed for this option to work. If NIS support is enabled, the portmap and ypbind services are started and are also enabled to start at boot time.

- Enable LDAP Support — Select this option to configure the system to retrieve user information via LDAP. Click the Configure LDAP button to specify the LDAP Search Base DN and LDAP Server. If Use TLS to encrypt connections is selected, Transport Layer Security is used to encrypt passwords sent to the LDAP server.

*The openldap-clients package must be installed for this option to work.

- Enable Hesiod Support — Select this option to configure the system to retrieve information from a remote Hesiod database, including user information.

*The hesiod package must be installed

22.2. Authentication

22.3. Command Line Version

```
#authconfig --help
#man authconfig
```

Option	*Description*
--enableshadow	Enable shadow passwords
--disableshadow	Disable shadow passwords
--enablemd5	Enable MD5 passwords
--disablemd5	Disable MD5 passwords
--enablenis	Enable NIS
--disablenis	Disable NIS
--nisdomain=<domain>	Specify NIS domain
--nisserver=<server>	Specify NIS server
--enableldap	Enable LDAP for user information
--disableldap	Disable LDAP for user information
--enableldaptls	Enable use of TLS with LDAP
--disableldaptls	Disable use of TLS with LDAP
--enableldapauth	Enable LDAP for authentication
--disableldapauth	Disable LDAP for authentication
--ldapserver=<server>	Specify LDAP server
--ldapbasedn=<dn>	Specify LDAP base DN
--enablekrb5	Enable Kerberos
--disablekrb5	Disable Kerberos
--krb5kdc=<kdc>	Specify Kerberos KDC
--krb5adminserver=<server>	Specify Kerberos administration server
--krb5realm=<realm>	Specify Kerberos realm
--enablesmbauth	Enable SMB
--disablesmbauth	Disable SMB
--smbworkgroup=<workgroup>	Specify SMB workgroup
--smbservers=<server>	Specify SMB servers
--enablehesiod	Enable Hesiod
--disablehesiod	Disable Hesiod

--hesiodlhs=<lhs> Specify Hesiod LHS
--hesiodrhs=<rhs> Specify Hesiod RHS
--enablecache Enable nscd
--disablecache Disable nscd
--nostart Do not start or stop the portmap, ypbind, or nscd services even if they are configured
--kickstart Do not display the user interface
--probe Probe and display network defaults

23. Mail Transport Agent (MTA) Configuration

#redhat-switch-mail
*Red Hat Linux 9 provides two MTAs: Sendmail and Postfix. If both are installed, sendmail is the default MTA.
#redhat-switch-mail-gnome
#redhat-switch-mail-nox ;Run in text mode
* The changes take place immediately

IV. System Configuration

24. Console Access

24.1. Disabling Shutdown Via Ctrl-Alt-Del

#cat /etc/inittab
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
Disable the ability-By putting a hash in front of it
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
OR: By putting -a flag to tell shutdown to look for the /etc/shutdown.allow file
ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
#cat /etc/shutdown.allow
stephen
jack
sophie
A list of usernames, one per line

24.2. Disabling Console Program Access

#rm -f /etc/security/console.apps/*
OR: Not allow any user at the console to run poweroff, halt, and reboot
#rm -f /etc/security/console.apps/poweroff
#rm -f /etc/security/console.apps/halt
#rm -f /etc/security/console.apps/reboot

24.3. Disabling All Console Access

- The PAM pam_console.so module manages console file permissions and authentication.
- Comment out all lines that refer to pam_console.so in the /etc/pam.d directory
- By this script:

```
cd /etc/pam.d
for i in * ; do
        sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

24.4. Defining the Consde

- The pam_console.so module uses the /etc/security/console.perms file to determine the permissions for users at the system console.

#cat /etc/security/console.perms
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
Define ttyS1:
#cat /etc/security/console.perms
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9] /dev/ttyS1

24.5. Making Files Accessible From the Console

1. #cat /etc/security/console.perms

```
<floppy>=/dev/fd[0-1]* \
        /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
        /dev/mixer* /dev/sequencer \
        /dev/sound/* /dev/beep
```

<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
#Added
<scanner>=/dev/scanner /dev/usb/scanner*

2. #cat /etc/security/console.perms
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound> 0640 root
<console> 0600 <cdrom> 0600 root.disk
#Added
<console> 0600 <scanner> 0600 root

24.6. Enabling Console Access for Other Applications

- Console access only works for applications which reside in /sbin or /usr/sbin, so the application that you wish to run must be there.

1. #cd /usr/bin
   #ln -s consolehelper foo
2. #touch /etc/security/console.apps/foo
3. #cp /etc/pam.d/halt /etc/pam.d/foo

** Now, when you run /usr/bin/foo, it will call consolehelper, which will authenticate the user with the help of /usr/sbin/userhelper. To authenticate the user, consolehelper will ask for the user's password if /etc/pam.d/foo is a copy of /etc/pam.d/halt (otherwise, it will do precisely what is specified in /etc/pam.d/foo) and then run /usr/sbin/foo with root permissions.*

- The PAM configuration file in etc/pam.d/ must include the following lines:
  auth sufficient /lib/security/pam_timestamp.so
  session optional /lib/security/pam_timestamp.so

** The first line that begins with auth should be after any other auth sufficient lines, and the line that begins with session should be after any other session optional lines.*

** By default, a successful authentication is cached for five minutes.*

24.7. The floppy Group

[root@bigdog root]# gpasswd -a fred floppy
Adding user fred to group floppy
[root@bigdog root]#

*Now, user fred will now be able to access the system's diskette drive from the console.

25. User and Group Configuration

- #redhat-config-users

25.1. Adding a New User

- Default: /bin/bash AND /home/<username>
- /etc/skel ;Default configuration files are copied into the new home directory
- User ID starting with number 500 will be assigned to the new user. Red Hat Linux reserves user IDs below 500 for system users.

25.2. Modifying User Properties

25.3. Adding a New Group

- Red Hat Linux reserves group IDs lower than 500 for system groups.

25.4. Modifying Group Properties

25.5. Command Line Configuration

1. Adding a User
   #useradd <username>
   #passwd <username>

Option	*Description*
-c comment	Comment for the user
-d home-dir	Home directory to be used instead of default /home/username
-e date	Date for the account to be disabled in the format YYYY-MM-DD

-f days — Number of days after the password expires until the account is disabled. (If 0 is specified, the account is disabled immediately after the password expires. If -1 is specified, the account will not be disabled after the password expires.)

-g group-name — Group name or group number for the user's default group (The group must exist prior to being specified here.)

-G group-list — List of additional (other than default) group names or group numbers, separated by commas, of which the user is a member. (The groups must exist prior to being specified here.)

-m — Create the home directory if it does not exist.

-M — Do not create the home directory.

-n — Do not create a user private group for the user.

-r — Create a system account with a UID less than 500 and without a home directory.

-p — password The password encrypted with crypt.

-s — User's login shell, which defaults to /bin/bash.

-u uid — User ID for the user, w hich must be unique and greater than 499.

2. Adding a Group

#groupadd <group-name>

Option	*Description*
-g gid	Group ID for the group, which must be unique and greater than 499.
-r	Create a system group with a GID less than 500.
-f	Exit with an error if the group already exists. (The group is not altered.) If -g and -f are specified, but the group already exists, the -g option is ignored.

3. Password Aging

#chage [options] <username>

Option	*Description*
-m days	Specify the minimum number of days between which the user must change passwords. If the value is 0, the password does not expire.
-M days	Specify the maximum number of days for which the password is valid. When the number of days specified by this option plus the number of days specified with the -d option is less than the current day, the user must change passwords before using the account.
-d days	Specify the number of days since January 1, 1970 the password was changed.
-I days	Specify the number of inactive days after the password expiration before locking the account. If the value is 0, the account is not locked after the password expires.
-E date	Specify the date on which the account is locked, in the format YYYY-MM-DD. Instead of the date, the number of days since January 1, 1970 can also be used.
-W days	Specify the number of days before the password expiration date to warn the user.

** Shadow passwords must be enabled to use the chage command.*

Lock the user's password

#usermod -L username

Force immediate password expiration

#chage -d 0 username

Unlock the account

There are two common approaches to this step.

1. To assign an initial password

#python

>(python)>>>import crypt; print crypt.crypt("password","salt")

* The output is the encrypted password similar to 12CsGd8FRcMSM.

Type [Ctrl]-[D] to exit the Python interpreter

usermod -p "encrypted-password" username ;Cut and paste the exact encrypted password output,

2. To assign a null password

#usermod -p "" username

**This process does not work if the user logs in using the SSH protocol.*

25.6. Explaining the Process

#useradd juan

1. A new line for juan is created in /etc/passwd. The line has the following characteristics:
- It begins with the username juan.
- There is an x for the password field indicating that the system is using shadow passwords.
- A UID at or above 500 is created. (Under Red Hat Linux, UIDs and GIDs below 500 are reserved for system use.)
- A GID at or above 500 is created.
- The optional GECOS information is left blank.
- The home directory for juan is set to /home/juan/.
- The default shell is set to /bin/bash.

2. A new line for juan is created in /etc/shadow. The line has the following characteristics:
- It begins with the username juan.
- Two exclamation points (!!) appear in the password field of the /etc/shadow file, which locks the account.
*If an encrypted password is passed using the -p flag, it is placed in the /etc/shadow file on the new line for the user.
- The password is set to never expire.

3. A new line for a group named juan is created in /etc/group. A group with the same name as a user is called a user private group. For more information on user private groups, refer to Section 25.1 Adding a New User.
The line created in /etc/group has the following characteristics:
- It begins with the group name juan.
- An x appears in the password field indicating that the system is using shadow group passwords.
- The GID matches the one listed for user juan in /etc/passwd.

4. A new line for a group named juan is created in /etc/gshadow. The line has the following characteristics:
- It begins with the group name juan.
- An exclamation point (!) appears in the password field of the /etc/gshadow file, which locks the group.
- All other fields are blank.

5. A directory for user juan is created in the /home/ directory. This directory is owned by user juan and group juan. However, it has read, write, and execute privileges only for the user juan. All other permissions are denied.

6. The files within the /etc/skel/ directory (which contain default user settings) are copied into the new /home/juan/ directory.

** At this point, a locked account called juan exists on the system. To activate it, the administrator must next assign a password to the account using the passwd command and, optionally, set password aging guidelines.*

26. Gathering System Information

26.1. System Processes

```
#ps aux | less
#ps ax | grep <running_process>
#top
```

Keys	*Description*
[Space]	Immediately refresh the display
[h]	Display a help screen
[k]	Kill a process. You will be prompted for the process ID and the signal to send to it.
[n]	Change the number of processes displayed. You will be prompted to enter the number.
[u]	Sort by user.
[M]	Sort by memory usage.
[P]	Sort by CPU usage.

**ps -m or type [Shift]-[H] in top => To view all threads, Not only the main (initial) thread.*

```
#gnome-system-monitor          ;For GNOME
```

26.2. Memory Usage

```
#free
#free -m                       ;Shown in megabyte
```

#gnome-system-monitor ;For GNOME

26.3. File Systems

#df
#df -h ;The -h argument stands for human-readable format.

*In the list of partitions, there is an entry for /dev/shm. This entry represents the system's virtual memory file system.

#du
#du -hs ;To see only the grand total for the directory in human-readable format
diskcheck ;The diskcheck RPM package have to be installed and run as an hourly cron task--It will send email to the system administrator.

#cat /etc/diskcheck.conf

```
defaultCutoff = 90
cutoff['/dev/hda3'] = 50
cutoff['/home'] = 50
exclude = "/dev/sda2 /dev/sda4"
ignore = "-x nfs -x iso9660"
mailTo = "webmaster@example.com"
mailFrom = "Disk Usage Monitor"
mailProg = "/usr/sbin/sendmail"
```

*Do not have to restart a service if you change the configuration file because it is read each time the cron task is run.

*/sbin/service crond status ;Should be start at boot time

26.4. Hardware

#hwbrowser
#lspci
#lspci -v ;for more verbose information or
#lspci -vv ;(Double V)for very verbose output

*The lspci is also useful to determine the networ k card in your system if you do not know the manufacturer or model number.

26.5. Additional Resources

man ps | top | du | df | lspci
Directory /proc

27. Printer Configuration

- For RH 9, the defaults to the CUPS printing system. The previous defaul t printing system, LPRng is still provided.

#redhat-config-printer
#command redhat-config-printer-tui ;For Text base
- /etc/printcap
- /etc/cups/
/etc/printcap.local ;For LPRng

The following types of print queues can be configured:

- Locally-connected — a printer attached directly to the computer through a parallel or USB port.
- Networked CUPS (IPP) — a printer that can be accessed over a TCP/IP network via the Internet Printing Protocol, also known as IPP (for example, a printer attached to another Red Hat Linux system running CUPS on the network).
- Networked UNIX (LPD) — a printer attached to a different UNIX system that can be accessed over a TCP/IP network (for example, a printer attached to another Red Hat Linux system running LPD on the network).
- Networked Windows (SMB) — a printer attached to a different system which is sharing a printer over a SMB network (for example, a printer attached to a Microsoft Windows machine).
- Networked Novell (NCP) — a printer attached to a different system which uses Novell's NetWare network technology.
- Networked JetDirect — a printer connected directly to the network through HP JetDirect instead of to a computer.

27.1. Adding a Local Printer

/dev/lp0 ;For a parallel printer
/dev/usb/lp0 ;For a USB printer

27.2. Adding an IPP Printer

- UDP port, 631 ;Open the port for Firewall

#redhat-config-printer
- Text fields for the following options appear:
Server — The hostname or IP address of the remote machine to which the printer is attached.
Path — The path to the print queue on the remote machine.

27.3. Adding a Remote UNIX (LPD) Printer

#redhat-config-printer
- Text fields for the following options appear:
Server — The hostname or IP address of the remote machine to which the printer is attached.
Queue — The remote printer queue. The default printer queue is usually lp.

27.4. Adding a Samba (SMB) Printer

#redhat-config-printer
- Click the Specify button on the right. Text fields for the following options appear:
Workgroup — The name of the Samba workgroup for the shared printer.
Server — The name of the server sharing the printer.
Share — The name of the shared printer on which you want to print. This name must be the same name defined as the Samba printer on the remote Windows machine.
User name — The name of the user you must log in as to access the printer. This user must exist on the Windows system, and the user must have permission to access the printer. The default user name is typically guest for Windows servers, or nobody for Samba servers.
Password — The password (if required) for the user specified in the User name field.

27.5. Adding a Novell NetWare (NCP) Printer

#redhat-config-printer
- Text fields for the following options appear:
Server — The hostname or IP address of the NCP system to which the printer is attached.
Queue — The remote queue for the printer on the NCP system.
User — The name of the user you must log in as to access the printer.
Password — The passw ord for the user specified in the User field above.

27.6. Adding a JetDirect Printer

#redhat-config-printer
- Text fields for the following options appear:
Printer — The hostname or IP address of the JetDirect printer.
Port — The port on the JetDirect printer that is listening for print jobs. The default port is 9100.

27.7. Selecting the Printer Model and Finishing

27.8. Printing a Test Page

27.9. Modifying Existing Printers

27.10. Saving the Configuration File

- /etc/cups directory (or the /etc/printcap file that lpd reads).
- To save printer configuration:
#/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
- To restore printer configuration:
#/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
- To merge the files:
#/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
- Must restart the printer daemon:
#/sbin/service cups restart ;For cups OR
#/sbin/service lpd restart ;For lpd

27.11. Command Line Configuration

1. Adding a Local Printer
#redhat-config-printer-tui --Xadd-local options
Options:
--device=node
(Required) The device node to use. For example, /dev/lp0.
--make=make
(Required) The IEEE 1284 MANUFACTURER string or the printer manufacturer's name as in the foomatic database if the manufacturer string is not available.
--model=model
(Required) The IEEE 1284 MODEL string or the printer model listed in the foomatic database if the model string is not available.
--name=name

(Optional) The name to be given to the new queue. If one is not given, a name based on the device node (such as "lp0") will be used.

--as-default

(Optional) Set this as the default queue.

#/sbin/service cups restart ;For cups OR
#/sbin/service lpd restart ;For lpd

2. Removing a Local Printer

#redhat-config-printer-tui --Xremove-local options

Options:

--device=node

(Required) The device node used such as /dev/lp0.

--make=make

(Required) The IEEE 1284 MANUFACTURER string, or (if none is available) the printer manufacturer's name as in the foomatic database.

--model=model

(Required) The IEEE 1284 MODEL string, or (if none is available) the printer model as listed in the foomatic database.

#/sbin/service cups restart ;For cups OR
#/sbin/service lpd restart ;For lpd
#/sbin/service cups stop ;For cups OR
#/sbin/service lpd stop ;For lpd

27.12. Managing Print Jobs

#lpq ;To view the list of print jobs in the print spool
#lpr sample.txt ;To print the text file sample.txt

27.13. Sharing a Printer

Sharing a Printer with LPRng

1. Create the file /etc/accepthost. In this file, add the IP address or hostname of the system that you want to allow print access to, with one line per IP or hostname.
2. Uncomment the following line in /etc/lpd.perms:

ACCEPT SERVICE=X REMOTEHOST=</etc/accepthost

3. Restart the daemon for the changes to take effect:

#service lpd restart

27.14. Switching Print Systems

#redhat-switch-printer
#redhat-switch-printer-nox ;For text mode

27.15. Additional Resources

man printcap — The manual page for the /etc/printcap printer configuration file.
map lpr — The manual page for the lpr command that allows you to print files from the command line.
man lpd — The manual page for the LPRng printer daemon.
man lprm — The manual page for the command line utility to remove print jobs from the LPRng spool queue.
man mpage — The manual page for the command line utility to print multiple pages on one sheet of paper.
man cupsd — The manual page for the CUPS printer daemon.
man cupsd.conf — The manual page for the CUPS printer daemon configuration file.
man classes.conf — The manual page for the class configuration file for CUPS.

28. Automated Tasks

- Use to perform periodic backups, monitor the system, run custom scripts, and more
- Four automated tasks utilities: cron, anacron, at, and batch

28.1. Cron

- vixie-cron RPM package installed

#rpm -q vixie-cron

- The crond service must be running

#cat /etc/crontab

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
# run-parts
01 * * * * root run-parts /etc/cron.hourly
```

02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly

SYNTAX:

* minute hour day month dayofweek command
  minute — any integer from 0 to 59
  hour — any integer from 0 to 23
  day — any integer from 1 to 31 (must be a valid day if a month is specified)
  month — any integer from 1 to 12 (or the short name of the month such as jan, feb, and so on)
  dayofweek — any integer from 0 to 7, where 0 or 7 represents Sunday (or the short name of the week such as sun, mon, and so on)
  command — the command to execute (The command can either be a command such as ls /proc >> /tmp/proc or the command to execute a custom script that you wrote.)
* An asterisk (*) can be used to specify all valid values
* A hyphen (-) between integers specifies a range of integers. For example, 1-4 means the integers 1, 2, 3, and 4.
* A list of values separated by commas (,) specifies a list. For example, 3, 4, 6, 8 indicates those four specific integers.
* The forward slash (/) can be used to specify step values. The value of an integer can be skipped within a range by following the range with /<integer>. For instance, the value */3 can be used in the month field to run the task every third month.

* Any lines that begin with a hash mark (#) are comments and are not processed
* If the MAILTO variable is defined as an empty string (MAILTO=""), email will not be sent.

- If a cron task needs to be executed on a schedule other than hourly, daily, weekly, or monthly, it can be added to the /etc/cron.d directory. All files in this directory use the same syntax as /etc/crontab.

- Users other than root can configure cron tasks by using the crontab utility. All user-defined crontabs are stored in the /var/spool/cron directory and are executed using the usernames of the users that created them. To create a crontab as a user, login as that user and type the command crontab -e to edit the user's crontab using the editor specified by the VISUAL or EDITOR environment variable. The file uses the same format as /etc/crontab. When the changes to the crontab are saved, the crontab is stored according to username and written to the file /var/spool/cron/username.

- The cron daemon checks the /etc/crontab file, the /etc/cron.d/ directory, and the /var/spool/cron directory every minute for any changes. If any changes are found, they are loaded into memory. Thus, the daemon does not need to be restarted if a crontab file is changed.

- Controlling Access to Cron
  - The /etc/cron.allow and /etc/cron.deny
  - The format of both access control files is one username on each line.

#/sbin/service crond <start,stop>

28.2. Anacron

- anacron RPM package installed
  #rpm -q anacron
- The anacron service must be running
  #/sbin/service anacron status
- Configuring Anacron Tasks
  #cat /etc/anacrontab

```
# /etc/anacrontab: configuration file for anacron
# See anacron(8) and anacrontab(5) for details.
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
# These entries are useful for a Red Hat Linux system.
1       5       cron.daily              run-parts /etc/cron.daily
7       10      cron.weekly             run-parts /etc/cron.weekly
30      15      cron.monthly            run-parts /etc/cron.monthly
```

SYNTAX:

period delay job-identifier command
period — frequency (in days) to execute the command
delay — delay time in minutes
job-identifier — description of the task, used in Anacron messages and as the name of the job's timestamp file, can contain any non-blank characters (except slashes)
command — command to execute

* /var/spool/anacron directory ;Records the date in a timestamp file

#/sbin/service anacron <start,stop>

28.3. At and Batch

- at RPM package installed
  # rpm -q at
- The atd service must be running
  #/sbin/service atd status
- Configuring At Jobs
  #at <time>
  at><command>[Enter]
  at><command>[Ctrl+D]
  HH:MM format — For example, 04:00 specifies 4:00AM. If the time is already past, it is executed at the specified time the next day.
  midnight — Specifies 12:00AM.
  noon — Specifies 12:00PM.
  teatime — Specifies 4:00PM.
  month-name day year format — For example, January 15 2002 specifies the 15th day of January in the year 2002. The year is optional.
  MMDDYY, MM/DD/YY, or MM.DD.YY formats — For example, 011502 for the 15th day of January in the year 2002.
  now + time — time is in minutes, hours, days, or weeks. For example, now + 5 days specifies that the command should be executed at the same time in five days.
  #cat /usr/share/doc/at-<version>/timespec ;For time syntax manual
- Configuring Batch Jobs
  - When the load average is below 0.8
  #batch
  at><command>[Enter]
  at><command>[Ctrl+D]
- To see the pending jobs (both at and batch)
  #atq
- If the set of commands or script tries to display information to standard out, the output is emailed to the user.
- Controlling Access to At and Batch
  - The /etc/at.allow and /etc/at.deny files
  - The format of both access control files is one username on each line.

#/sbin/service atd <start,stop>

28.4. Additional Resources

man cron | contab | anacron | anacrontab | at
/usr/share/doc/at-<version>/timespec
/usr/share/doc/anacron-<version>/README

29. Log Files

29.1. Locating Log Files
29.2. Viewing Log Files
29.3. Examining Log Files

30. Upgrading the Kernel

30.1. The 2.4 Kernel

Features:

The directory for the kernel source is /usr/src/linux-2.4/ instead of /usr/src/linux/.
Support for the ext3 file system.
Multi-processor (SMP) support.
USB support.
Preliminary support for IEEE 1394, also referred to as FireWire, devices

30.2. Preparing to Upgrade

1. Make sure a working boot diskette exists for the system in case a problem occurs
   #/sbin/mkbootdisk `uname -r`
2. Reboot the machine with the boot diskette and verify that it works before continuing
3. To determine which kernel packages are installed
   #rpm -qa | grep kernel
   kernel-2.4.20-2.47.1

kernel-debug-2.4.20-2.47.1
kernel-source-2.4.20-2.47.1
kernel-doc-2.4.20-2.47.1
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.20-2.47.1

4. Determine which packages need to be download for the kernel upgrade:
- The only required package is the kernel package for a single processor system.
- The kernel-smp package is for the computer has more than one processor.
- The kernel-bigmem package must be installed for the system to use more than four gigabytes of memory.
- If PCMCIA support is needed (such as on a laptop), the kernel-pcmcia-cs package is necessary.
- kernel-2.4.20-2.47.1.athlon.rpm is optimized for AMD Athlon and AMD Duron systems and kernel-2.4.20-2.47.1.i686.rpm is optimized for Intel Pentium II, Intel Pentium III, and Intel Pentium 4 systems.

30.3. Downloading the Upgraded Kernel

30.4. Performing the Upgrade

```
#rpm -ivh kernel-2.4.20-2.47.1.i386.rpm
#rpm -ivh kernel-smp-2.4.20-2.47.1.i386.rpm                ;For multi processor
#rpm -ivh kernel-bigmem-2.4.20-2.47.1.i686.rpm             ;If the system is i686-based and contains more than 4 gigabytes of RAM
#rpm -Uvh kernel-source-2.4.20-2.47.1.i386.rpm             ;For kernel sources
#rpm -Uvh kernel-docs-2.4.20-2.47.1.i386.rpm               ;For kernel document
#rpm -Uvh kernel-utils-2.4.20-2.47.1.i386.rpm              ;For kernel utilities
#rpm -ivh –force kernel-pcmcia-cs-3.1.24-2.i386.rpm        ;Use --force if it returns a conflict
```

30.5. Verifying the Initial RAM Disk Image

- If the system uses the ext3 file system or a SCSI controller, an initial RAM disk is needed.
- The purpose of the initial RAM disk is to allow a modular kernel to have access to modules that it might need to boot from before the kernel has access to the device where the modules normally reside.
- The initial RAM disk can be created with the mkinitrd command

```
#mkinitrd                                                  ;This step is performed automatically if the kernel is installed from the RPM package.
```

- Verify by:

```
#ls -l /boot
initrd-2.4.20-2.47.1.img                                   ;The version should match the version of the kernel just installed
```

30.6. Verifying the Boot Loader

- It does not configure the boot loader to boot the new kernel by default.

- GRUB:

```
#cat /boot/grub/grub.conf
    #boot=/dev/hda
    default=1
    timeout=10
    splashimage=(hd0,0)/grub/splash.xpm.gz
    title Red Hat Linux (2.4.20-2.47.1)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.47.1 ro root=LABEL=/
        initrd /initrd-2.4.20-2.47.1.img
    title Red Hat Linux (2.4.20-2.30)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30 ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.img
```

* Must contains a title section with the same version as the kernel package just installed
* The default is not set to the new kernel:
    - Change the value of the default variable to point to the title section of new kernel: (The first section number = 0)

- LILO:

```
#cat /etc/lilo.conf
    prompt
    timeout=50
    default=2.4.20-2.30
    boot=/dev/hda
    map=/boot/map
    install=/boot/boot.b
```

```
message=/boot/message
linear

image=/boot/vmlinuz-2.4.20-2.47.1
label=2.4.20-2.47.1
initrd=/boot/initrd-2.4.20-2.47.1.img
read-only
append="root=LABEL=/"

image=/boot/vmlinuz-2.4.20-2.30
label=2.4.20-2.30
initrd=/boot/initrd-2.4.20-2.30.img
read-only
append="root=LABEL=/"
```

** The default is not set to the new kernel*
** Set the default variable to the value of label in the image section for the new kernel*

```
#/sbin/lilo
        Added 2.4.20-2.47.1 *
        Added linux
```

31. Kernel Modules

- /etc/modules.conf ;The module configuration file
- Video card modules used to display the X Window System interface are part of the XFree86 package: not kernel package.

31.1. Kernel Module Utilities

#/sbin/lsmod ;Displays a list of currently loaded modules AND the same as /proc/modules

```
Module                  Size  Used by    Not tainted
iptable_filter          2412  0 (autoclean) (unused)
ip_tables      15864    1 [iptable_filter]
nfs            84632    1 (autoclean)
lockd          59536    1 (autoclean) [nfs]
sunrpc         87452    1 (autoclean) [nfs lockd]
soundcore               7044  0 (autoclean)
ide-cd         35836    0 (autoclean)
cdrom          34144    0 (autoclean) [ide-cd]
parport_pc              19204 1 (autoclean)
lp             9188     0 (autoclean)
parport        39072    1 (autoclean) [parport_pc lp]
autofs         13692    0 (autoclean) (unused)
e100           62148    1
microcode               5184  0 (autoclean)
keybdev                 2976  0 (unused)
mousedev                5656  1
hid            22308    0 (unused)
input          6208     0 [keybdev mousedev hid]
usb-uhci       27468    0 (unused)
usbcore                 82752 1 [hid usb-uhci]
ext3           91464    2
jbd            56336    2 [ext3]
```

- The first column is the name of the module, the second column is the size of the module, and the third column is the use count.
- If (unused) is listed on the line for the module, the module is currently not being used.
- *If (autoclean) is on the line for the module, the module can be autocleaned by the rmmod -a command. When this command is executed, any modules that are tagged with autoclean, that have not been used since the previous autoclean action, are unloaded.

- Red Hat Linux does not perform this autoclean action by default.
- If a module name is listed at the end of the line in brackets, the module in the brackets is dependent on the module listed in the first column of the line.

#/sbin/modprobe <kernel_module_name> ;To load a kernel module

- Attempts to load the module from the /lib/modules/<kernel-version>/kernel/drivers/ subdirectories.

#/sbin/modprobe -v hid ;To print to the screen all commands: To show commands loading the other modules

/sbin/insmod /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.20-2.47.1/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'

- The /sbin/insmod command also exists to load kernel modules; however, it does not resolve dependencies. Thus, it is recommended that the /sbin/modprobe command be used.

#/sbin/rmmod hid ;To unload kernel modules: option -a for all
#sbin/modinfo [options] <module> ;To display information about a kernel module
Options -d = displays a brief description of the module
Options -p = lists the parameters the module supports

31.2. Additional Resources

man lsmod | insmod | modprobe | modinfo
/usr/src/linux-2.4/Documentation/modules.txt

V. Package Management

32. Package Management with RPM

32.1. RPM Design Goals

32.2. Using RPM

Installing
#rpm -Uvh foo-1.0-1.i386.rpm

Package Already Installed
#rpm -ivh –replacepkgs foo-1.0-1.i386.rpm

Conflicting Files
#rpm -ivh –replacefiles foo-1.0-1.i386.rpm

Unresolved Dependency
#rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
#rpm -q --redhatprovides bar.so.2

Uninstalling
#rpm -e foo

Upgrading
#rpm -Uvh foo-2.0-1.i386.rpm
#rpm -Uvh --oldpackage foo-1.0-1.i386.rpm

Freshening
#rpm -Fvh foo-1.2-1.i386.rpm
#rpm -Fvh *.rpm

Querying
#rpm -q foo

Verifying
#rpm -Vf /bin/vi ;To verify a package containing a particular file:
#rpm -Va ;To verify ALL installed packages:
#rpm -Vp foo-1.0-1.i386.rpm ;To verify an installed package against an RPM package file:

32.3. Checking a Package's Signature

32.4. Impressing Your Friends with RPM

You may find a new RPM, but you do not know what it does. To find information about it, use the following command:

#rpm -qip crontabs-1.10-5.noarch.rpm

Perhaps you now want to see what files the crontabs RPM installs. You would enter the following:

#rpm -qlp crontabs-1.10-5.noarch.rpm

32.5. Additional Resources

man rpm

rpm --help

33. Package Management Tool

33.1. Installing Packages
33.2. Removing Packages

34. Red Hat Network

VI. Appendixes

A. Building a Custom Kernel

A.1. Preparing to Build

```
#/sbin/mkbootdisk `uname -r`                    ;Make a rescue disk
#rpm -q kernel-source                           ;The kernel-source package must be installed
```

A.2. Building the Kernel

1. Open a shell prompt and change to the directory /usr/src/linux-2.4/.

2. Remove any configuration files along with the remains of any previous builds that may be scattered around the source tree.

```
#cp /usr/src/linux-2.4/.config ~root/tmp/      ;Backup
#make mrproper
#cp ~root/tmp/.config /usr/src/linux-2.4/      :Restore .config file
```

3. The default Red Hat Linux kernel should be used as a starting point.

```
#cp /usr/src/linux-2.4/configs/config  /usr/src/linux-2.4/.config.
```

4. Customize the settings

```
#make xconfig                                  ;The tk package must be installed.
```

Other available methods for kernel configuration include

```
#make config
#make menuconfig
#make oldconfig
```

To use kmod and kernel modules answer Yes to kmod support and module version (CONFIG_MODVERSIONS) support during the configuration

5. Set up the dependencies correctly after creating a /usr/src/linux-2.4/.config file

```
#make dep
```

6. Prepare the source tree for the build

```
#make clean
```

7. The custom kernel have a modified version number so that the existing kernel is not overwritten. By default, /usr/src/linux-2.4/Makefile includes the word custom at the end of the line beginning with EXTRAVERSION.

* Appending the string allows the system to have the old working kernel and the new kernel (version 2.4.20-2.47.1custom) on the system at the same time.

8. Build the kernel

```
#make bzImage
```

9. Build any modules configured

```
#make modules
```

10.Install the kernel modules (even if nothing was actually built): This installs the kernel modules into the directory path /lib/modules/<KERNELVERSION>/kernel/drivers (where KERNELVERSION is the version specified in the Makefile).

```
#make modules_install
#ls -la /lib/modules/2.4.20-2.47.1custom/kernel/drivers/
```

11.Copy the new kernel and its associated files to the proper directories:

#make install

* To installing the kernel files in the /boot directory: AND

* Executes the /sbin/new-kernel-pkg script that builds a new initrd image and adds new entries to the boot loader configuration file.

* The initrd image is required If the system has a SCSI adapter and the SCSI driver was compiled as a module or if the kernel was built with ext3 support as a module.

12.Even though the initrd image and boot loader modifications are made, verify that they were done correctly and be sure to use the custom kernel version instead of 2.4.20-2.47.1.

A.3. Building a Monolithic Kernel

To build a monolithic kernel, follow the same steps as building a modularized kernel, with a few exceptions.

1. When configuring the kernel, do not compile anything as a module. In other words, only answer Yes or No to the questions. Also, answer No to kmod support and module version (CONFIG_MODVERSIONS) support.

2. Omit the following steps:

make modules

make modules_install

3. Append the kernel line in grub.conf with nomodules or edit lilo.conf to include the append=nomodules line.

A.4. Additional Resources

/usr/src/linux-2.4/Documentation

B. Getting Started with Gnu Privacy Guard