**Questions 1 | CREATE LVM**  
Create the "LVM" with the name "source" by using 26PE's from the volume group "open". Consider the PE size as "8MB". Mount it on /mnt/secret with filesystem vfat.  
  
**Questions 2 | USER'S GROUPS AND PERMISSION:**  
Create a group named "sysadmin" A user sarah and natasha should belongs to "manager" group as a secondary group . A user harry should not have access to interactive shell and he should not be a member of "manager" group. passwd for all user created should be "password".  
  
**Questions 3 | DIRECTORY COLLABORATION:**  
Create the Directory "/home/manager" with the following characteristics. Group ownership of "/home/manager" should go to "manager" group. The directory should be have full permission for all members off "manager" group but not to any other users accept "root". Files created under "/home/manager" should get the same group ownership is set to the "manager" group.  
  
**Questions 4 | UPDATE THE KERNEL:**  
Install the appropriate Kernel from<ftp://instructor.example.com/ftp/updates>. Your machine should boot with updated kernel.  
**Questions 5 | CRON JOB:**  
The user sarah must configure a cron job that runs today at 14:23 today. and executes "/bin/echo "hyer" and deny the user max for creating cronjob .  
**Questions 6 | RESIZE LVM:**  
Resize the lvm "/dev/vgsrv/home" (/dev/myvol/vo) so that after reboot size should be in between 90MB to 120MB..  
**Questions 7 | BIND THE "LDAP" FOR USER AUTHENTICATION:**  
Note the following. BASE DN: dc=example,dc=com ldap path ldap://instructor.example.com/ Download the certificate from "<ftp://instructor.example.com/pub/EXAMPLE-CA-CERT>"Ldap user should login into your system . Where "X" is your system no.  
  
**Questions 8 | "NTP" CLIENT:**  
Configure your system as "NTP" client for "instructor.example.com".  
  
**Questions 9 | AUTOMOUNT THE HOME DIRECTORY FOR LDAPUSER**  
Note the following. instructor.example.com(192.168.0.254) "Nfs exports" /home/guests to your system where "x" is your station ip. Ldapuser's home directory is instructor.example.com:/home/guests/ldapuserx. Ldapuser's home directory should be automounted locally beneath at /home/guests/ldapuserx. While login with any of the ldapuser then only home directory should accesible from your system that ldapuserx.  
**Questions 10 | ACCESS CONTROL LIST:**  
Copy the file /etc/fstab to /var/tmp and configure the "ACL" as mention following. The file /var/tmp/fstab is owned by the "root". The file /var/tmp/fstab belongs to the group "root" The file /var/tmp/fstab should not be executable by other's. The user "sarah" should able to read and write to the file. The user "natasha" can neither read nor write to the file. other users (future and current) shuold be able to read /var/tmp/fstab. Create a directory /data ,set default group as ftp so that when content will be created under this dir group ftp will be inherited.  
  
**Questions 11 | CONFIGURE FTP SERVER:**  
Configure FTP access from your system. Clients within the remote.test should not have anonomyous FTP access to your system.  
  
**Questions 12 | CONFIGURE "web server":**  
Configure your system as "web server" for the site[http://serverX.example.com](http://serverx.example.com/) . Download the web page from<ftp://instructor.example.com/updates/station.html> Rename the the downloaded page as "index.html" Copy the "index.html" page to the "document root" Do not make any modifications to the content of index.html.  
  
**Questions 13 | ADD USERS:**  
Create the user "dax" with uid 4223.  
  
**Questions 14 | EXTEND SWAP SPACE:**  
Extend the SWAP space with "250" MB dont remove the existing swap.  
  
**Questions 15 | LOCATE THE FILES:**  
locate the files of owner "dax" and copy to the directory /root/found directory  
  
**Questions 16 | SEARCH FOR WORD:**  
List all lines which have string "full" from "/usr/share/dict/words" file and copy the lines in /root/word.found.

Hello all,  
  
I passed on friday my EX200 or RHCSA exam with 300 points.  
  
My study materials Michael Jang and VTC RHCSA videos,  but think this is a bit too much theory, I would prefer various RHCSA exam question/ blogs which can be found on the internet in the first place. those books like Michael Jang and VTC are time killers  
  
I wil try to put all text stuff that I used for study in the section share.  
  
Still there are several points which you must know to pass:  
  
1. Reset roots pwd  - single user mode  
  
2. Working with LVM  
  
3. Working with fdisk also recommend cfdisk, saved my a..s  
  
4. creating users, groups, acl, crontab  
  
5. Autofs, and ldap client  
  
6. Configure a custom repo f.e for http, install kernel,  - I found pretty good lynx for a guestion  
  
7. Install HTTPd, Vsftpd  
  
  
  
Kind regards  
  
  
Hi  
  
my comments, notice that there can be differences, dont know how many scenarios are out there  
  
Notice dont forget to test you configuration with a reboot!!!!  
  
Check how to configure a repo for http/ftp server  
  
Configure network with system-config-network/tui, and be sure it works after reboot!!!!!!  
I had a issue had to set NM to yes,  
  
Yes almost forgot, it is also essential to know how to reset roots pwd on a unknow system, where you simply dont know the previous roots pwd,  
  
just at boot type a and type 1 and boot system in single user mode and reset roots pwd, to that you will have to use at your exam  
  
**Questions 1 | CREATE LVM**  
Create the "LVM" with the name "source" by using 26PE's from the volume group "open". Consider the PE size as "8MB". Mount it on /mnt/secret with filesystem vfat.  
--> notice here that the already 3 partition present vda1,2,3 I had two question 1st was to create a swap from partition (NOT from LVM) and 2nd was to create a new LVM with new VG and new LV. Since you cant have 5 primary partition you need to create the next 5 partition as logical, recommend doing this with cfdisk, had issues rereading new partitions using partx -a, or partprobe, in some cases I had to reboot the server  
  
**Questions 2 | USER'S GROUPS AND PERMISSION:**  
Create a group named "sysadmin" A user sarah and natasha should belongs to "manager" group as a secondary group . A user harry should not have access to interactive shell and he should not be a member of "manager" group. passwd for all user created should be "password".  
--> This task can differ  with names, but the task I had was similiar  
  
**Questions 3 | DIRECTORY COLLABORATION:**  
Create the Directory "/home/manager" with the following characteristics. Group ownership of "/home/manager" should go to "manager" group. The directory should be have full permission for all members off "manager" group but not to any other users accept "root". Files created under "/home/manager" should get the same group ownership is set to the "manager" group.  
--> this also pretty ease you need to set g+s on the directory  
  
**Questions 4 | UPDATE THE KERNEL:**  
Install the appropriate Kernel from<ftp://instructor.example.com/ftp/updates>. Your machine should boot with updated kernel.  
--> I think I had the kernel on a http location used lynx  to get the exact path to the new kernel and kernel-firmware, used after wget to download it. use rpm -vih kernel-firmware and then rpm -ivh kermel dont do -Uvh, this will remove the previous kernel, no changes are needed.  
--> if the source is ftp just ftp and open or lftp  
  
  
**Questions 5 | CRON JOB:**  
The user sarah must configure a cron job that runs today at 14:23 today. and executes "/bin/echo "hyer" and deny the user max for creating cronjob .  
--> yes this matches, but had it without the deny  
  
**Questions 6 | RESIZE LVM:**  
Resize the lvm "/dev/vgsrv/home" (/dev/myvol/vo) so that after reboot size should be in between 90MB to 120MB..  
Yup, if you are not sure make a copy of the /home, or where the LV points to. so umount > fsck > resize /dev.../lv 100M > lvresize -L 100M /dev. (by lvresize you may get a message about destroying your data just confirm).., dont change the order lvresize and resize,  
  
**Questions 7 | BIND THE "LDAP" FOR USER AUTHENTICATION:**  
Note the following. BASE DN: dc=example,dc=com ldap path ldap://instructor.example.com/ Download the certificate from "<ftp://instructor.example.com/pub/EXAMPLE-CA-CERT>"Ldap user should login into your system . Where "X" is your system no.  
  
--> Yes this is pretty easy, just start from GUI the Authentification Tool or authconfig/authconfig-tui  
If all goes well verify changes with getend passwd ldapuser01  
  
**Questions 8 | "NTP" CLIENT:**  
Configure your system as "NTP" client for "instructor.example.com".  
--> yes done with system-configure-date or time dont know the exact name, can be also found in the system tools  
  
  
**Questions 9 | AUTOMOUNT THE HOME DIRECTORY FOR LDAPUSER**  
Note the following. instructor.example.com(192.168.0.254) "Nfs exports" /home/guests to your system where "x" is your station ip. Ldapuser's home directory is instructor.example.com:/home/guests/ldapuserx. Ldapuser's home directory should be automounted locally beneath at /home/guests/ldapuserx. While login with any of the ldapuser then only home directory should accesible from your system that ldapuserx.  
--> Yes matches,  
create a copy from auto.misc called auto.ldap  
in ldap comment all and type the following  
/home/guests auto.ldap  
  
in the auto.ldap  
ldapuser01 -fstype=nfs IP:/home/quests/ldapuser01 --> nfs is NFSv3  
\* -fstype=nfs IP:/home/quests/& --> all users  
  
**Questions 10 | ACCESS CONTROL LIST:**  
Copy the file /etc/fstab to /var/tmp and configure the "ACL" as mention following. The file /var/tmp/fstab is owned by the "root". The file /var/tmp/fstab belongs to the group "root" The file /var/tmp/fstab should not be executable by other's. The user "sarah" should able to read and write to the file. The user "natasha" can neither read nor write to the file. other users (future and current) shuold be able to read /var/tmp/fstab. Create a directory /data ,set default group as ftp so that when content will be created under this dir group ftp will be inherited.  
--> matches, just use setfacl -m u:user:rwx file, verify with getfacl, or simply switch to users and try to make changes  
  
**Questions 11 | CONFIGURE FTP SERVER:**  
Configure FTP access from your system. Clients within the remote.test should not have anonomyous FTP access to your system.  
Yes, notice, you must configure you network connection!  
yum install vsftpd  
chkconfig vsftpd on  
service vsftpd start  
Didnt had the second part, with deny just that anonymous users should have access  
  
  
**Questions 12 | CONFIGURE "web server":**  
Configure your system as "web server" for the site[http://serverX.example.com](http://serverx.example.com/) . Download the web page from<ftp://instructor.example.com/updates/station.html> Rename the the downloaded page as "index.html" Copy the "index.html" page to the "document root" Do not make any modifications to the content of index.html.  
Similiar installation as vsftpd packege name is httpd  
  
Dont forget to configure /etc/httpd/conf/httpd.conf  
NameVirtualHost XX:80  
<VirtualHost XX:80>  
DocumentRoot /var/www/html/  
ServerName station.domainXX.example.com  
</VirtualHost>  
  
**Questions 13 | ADD USERS:**  
Create the user "dax" with uid 4223.  
--> ok  
  
**Questions 14 | EXTEND SWAP SPACE:**  
Extend the SWAP space with "250" MB dont remove the existing swap.  
--> yes check first questions and create new logical/extended partition  
  
**Questions 15 | LOCATE THE FILES:**  
locate the files of owner "dax" and copy to the directory /root/found directory  
--> yes, find / -user dax -exec cp -prf {} /dest\_folder/ \;  
  
**Questions 16 | SEARCH FOR WORD:**  
List all lines which have string "full" from "/usr/share/dict/words" file and copy the lines in /root/word.found.   
--> simply todo for grep

**Questions 1 | CREATE LVM**   
Create the "LVM" with the name "source" by using 26PE's from the volume group "open". Consider the PE size as "8MB". Mount it on /mnt/secret with filesystem vfat.  
  
**Questions 2 | USER'S GROUPS AND PERMISSION:**   
Create a group named "sysadmin" A user sarah and natasha should belongs to "manager" group as a secondary group . A user harry should not have access to interactive shell and he should not be a member of "manager" group. passwd for all user created should be "password".  
  
**Questions 3 | DIRECTORY COLLABORATION:**   
Create the Directory "/home/manager" with the following characteristics. Group ownership of "/home/manager" should go to "manager" group. The directory should be have full permission for all members off "manager" group but not to any other users accept "root". Files created under "/home/manager" should get the same group ownership is set to the "manager" group.  
  
**Questions 4 | UPDATE THE KERNEL:**   
Install the appropriate Kernel from <ftp://instructor.example.com/ftp/updates>. Your machine should boot with updated kernel.  
**Questions 5 | CRON JOB:**   
The user sarah must configure a cron job that runs today at 14:23 today. and executes "/bin/echo "hyer" and deny the user max for creating cronjob .  
**Questions 6 | RESIZE LVM:**   
Resize the lvm "/dev/vgsrv/home" (/dev/myvol/vo) so that after reboot size should be in between 90MB to 120MB..  
**Questions 7 | BIND THE "LDAP" FOR USER AUTHENTICATION:**   
Note the following. BASE DN: dc=example,dc=com ldap path ldap://instructor.example.com/ Download the certificate from "<ftp://instructor.example.com/pub/EXAMPLE-CA-CERT>"Ldap user should login into your system . Where "X" is your system no.  
  
**Questions 8 | "NTP" CLIENT:**   
Configure your system as "NTP" client for "instructor.example.com".  
  
**Questions 9 | AUTOMOUNT THE HOME DIRECTORY FOR LDAPUSER**   
Note the following. instructor.example.com(192.168.0.254) "Nfs exports" /home/guests to your system where "x" is your station ip. Ldapuser's home directory is instructor.example.com:/home/guests/ldapuserx. Ldapuser's home directory should be automounted locally beneath at /home/guests/ldapuserx. While login with any of the ldapuser then only home directory should accesible from your system that ldapuserx.  
**Questions 10 | ACCESS CONTROL LIST:**   
Copy the file /etc/fstab to /var/tmp and configure the "ACL" as mention following. The file /var/tmp/fstab is owned by the "root". The file /var/tmp/fstab belongs to the group "root" The file /var/tmp/fstab should not be executable by other's. The user "sarah" should able to read and write to the file. The user "natasha" can neither read nor write to the file. other users (future and current) shuold be able to read /var/tmp/fstab. Create a directory /data ,set default group as ftp so that when content will be created under this dir group ftp will be inherited.  
  
**Questions 11 | CONFIGURE FTP SERVER:**   
Configure FTP access from your system. Clients within the remote.test should not have anonomyous FTP access to your system.  
  
**Questions 12 | CONFIGURE "web server":**   
Configure your system as "web server" for the site <http://serverX.example.com> . Download the web page from <ftp://instructor.example.com/updates/station.html> Rename the the downloaded page as "index.html" Copy the "index.html" page to the "document root" Do not make any modifications to the content of index.html.  
  
**Questions 13 | ADD USERS:**   
Create the user "dax" with uid 4223.  
  
**Questions 14 | EXTEND SWAP SPACE:**   
Extend the SWAP space with "250" MB dont remove the existing swap.  
  
**Questions 15 | LOCATE THE FILES:**   
locate the files of owner "dax" and copy to the directory /root/found directory  
  
**Questions 16 | SEARCH FOR WORD:**   
List all lines which have string "full" from "/usr/share/dict/words" file and copy the lines in /root/word.found.

**RHCSA Exam**  
  
**Please login to your system as root, SELinux must be running in the Enforcing mode.**  
  
**Q1: Configure your host name to be stationX.redhat.com**.  
  
**Q2: Create the following users, groups, and group memberships:**

* A group named sysusers
* A user andrew who belongs to sysusers as a secondary group
* A user susan who also belongs to sysusers as a secondary group
* A user brad who does not have access to an interactive shell on the system, and who is not a member of sysusers
* andrew, susan, and brad should all have the password of Rhel#6

**Q3: Create a collaborative directory /shared/sysusers with the following characteristics:**

* Group ownership of /shared/sysusers is sysusers
* The directory should be readable, writable, and accessible to members of sysusers, but not to any other user. (It is understood that root has access to all files and directories on the system.)
* Files created in /shared/sysusers automatically have group ownership set to the sysusers group

**Q4: Set up the default local print queue to forward jobs to the IPP (CUPS) print queue stationx on server.redhat.com, where x is your station number. Configure this printer as a “Generic – text- only” print queue.**  
**Note: The queue stationx on server dumps print jobs into the file** [**http://server/printers/stationx.**](http://server/printers/stationx.) **This file can be examined to confirm that you have configured the print queue correctly.**  
  
**Q5: The user andrew must configure a cron job that**

* runs daily at 15:25 local time and executes /bin/echo hello
* he is the only one whom con use cron

**Q6: Bind to the LDAP domain redhat.com provided by 192.168.1.254 for user authentication. Note the following:**

* guest01x should be able to log into your system, where x is your station number, but will not have a home directory until you have completed the autofs requirement below
* you can find LDAP certificate on <http://server.redhat.com/redhat.cert>
* All LDAP users have a password of redhat

**Q7: Configure autofs to automount the home directories of LDAP users. Note the following:**

* server.redhat.com (192.168.1.254) NFS-exports /rhome to your system, where x is your station number
* guest01x home directory is server.redhat.com:/rhome/guest01x
* guest01x home directory should be automounted locally beneath /exports
* home directories must be writable by their users
* While you are able to log in as any of the users guest012 through guest019, the only home directory that is accessible from your system is guest01x.

**Example:** station10 would configure the automounter such that guest011’s home directory /exports/guest011 gets mounted automatically upon login. The NFS share would be server.redhat.com:/rhome/guest011.  
  
**Q8: Copy the file /etc/fstab to /var/tmp. Configure the permissions of /var/tmp/fstab so that:**

* the file /var/tmp/fstab is owned by the root user.
* the file /var/tmp/fstab belongs to the group root.
* the file /var/tmp/fstab should not be executable by anyone.
* the user andrew is able to read and write /var/tmp/fstab.
* the user susan can neither write nor read /var/tmp/fstab.
* all other users (current or future) have the ability to read /var/tmp/fstab.

**Q9: Configure your system so that:**

* it is an NTP client of server.redhat.com
* yum is configured to find the rpm pakages locally from the cdrom on your system

**Q10: Configure FTP access on your system:**

* Clients within the redhat.com domain should have anonymous FTP access to your machine
* FTP is listening on port 2121

**Q11: Implement a web server for the site** [**http://stationX.redhat.com**](http://stationX.redhat.com)**, then perform the following steps:**

* Download <ftp://server.redhat.com/pub/rhce/station.html>
* Rename the downloaded file to index.html
* Copy this index.html to the DocumentRoot of your web server
* Do NOT make any modifications to the content of index.html

**Q12: One Logical Volume is should be created named as myvol under vo volume group and is mounted to /data. The Initial Size of that Logical Volume is 124MB.**  
  
**Q13: if applicable, resize your home directory to be 200M.**  
  
**Q14: find All files that had been modified before 11 March and save them under /modified**.  
  
**BQ: write a script to find the user who made the last login failure on the system using ssh.**

**Its a Request to a LINUX Friendlier to have the Step Provided in Screen-shorts**  
  
  
  
01. Login to server X as root.  
  
02. Create an archive of /etc using gzip compression. Save the file as  
/tmp/etc.tar.gz.  
  
03. Copy the /tmp/etc.tar.gz file from your server X to the /backup directory on  
your desktop X machine.  
  
04. Extract the compressed archive to /backup on desktop X.  
  
05. Print all usernames that begin with the letter r.  
  
06. Print all usernames that begins with the letter g.  
  
07. Print all accounts whose shells (last column) are /sbin/nologin  
  
08. Print all accounts that have a UID or GID (third or fourth columns) of O.  
  
09. Print all accounts that have a UID or GID in the range of 10-19.  
  
10. List all files in /usr/share/doc that end with the number four.  
  
11. Print all lines in /etc/hosts that have a number in them.  
  
12. Print the line in /etc/hosts that has a 127.0.0.1  
  
13. Run the following command as student, and redirect STDOUT to /tmp/output.txt  
and redirect STDERR to /tmp/error.txt.  
  
14. Run the following command as student, and redirect both STDOUT and STDERR to  
the /tmp/all.txt file.  
  
15. Sort the /etc/passwd file and send it to the default printer  
  
16. Print out lines in /etc/passwd that have a three digit number between colons  
(file:///C:%5CUsers%5CJOY%5CAppData%5CLocal%5CTemp%5Cmsohtmlclip1%5C01%5Cclip\_image001.gif  
  
17. a. What is its current IP Address?  
  
b. What is its current CIDR subnet mask?  
c. What is its current default gateway?  
d. What is its current hostname?  
e. What are its current DNS servers?  
  
18. Run the first script to mis-configure your networking:  
Lab-break-net 1  
  
19. Symptom: A web browser is unable to access the web page at   
Code:  
  
<http://instructor.remote.test>  
20. Apply the three steps: TEST, CHECK, FIX to identify and resolve the problem.  
  
21. Run the second script to mis-configure your networking:  
Lab-break-net 2  
  
22. Symptom: A web browser is unable to access the web page at   
Code:  
  
<http://instructor.remote.test>  
23. Apply the three steps: TEST, CHECK, FIX to identify and resolve the3 problem.  
  
24. Create a new partition and ext4 file system that is 400 MB in size. The file  
system should persistently mount under /data.  
  
25. Persistently and a swap partition that is 200 MB in size.  
  
26. Create a volume group called vg1 of 500 MB on serverX.  
Create a logical volume called lv1 of 200 MB on vg1.  
  
Format the logical volume with ext4 and mount it under /data.  
  
  
  
  
  
27. Create a group called sysadmin.  
  
Create two users called u1 and u2 and set the password to redhat.  
sysadmin should be the secondary group of u1 and u2.  
Create another user called guest who is not a member of sysadmin and who  
should not have any login shell.  
  
28. Create a directory called /database whose group owner should be sysadmin.  
Sysadmin group member should have full access on /database and others should  
have no access on it.  
  
29. Schedule a cron job for u1, so that a disk free report is mailed to u2 every  
day at 7:30 p.m.  
  
30. You will now set up the automounter to automatically mount an NFS export on a  
specified direct5ory on demand.  
• The NFS server is [instructor.example.com](http://instructor.example.com)  
• The NFS export on the server is /var/ftp/pub  
• The automatic mount point on your station should be /server/public  
• Use an indirect map (not /net) to implement this  
• Validate that the automount works by changing directory to the mount point and accessing the files in the share.  
  
Perform the following steps:  
1. Create/modify autofs service configuration files.  
2. Reload the automounter.  
3. Access the share.  
  
31. Using ACLs to Grant and Limit Access  
  
This lab uses users and groups created earlier on server X. If you do not  
already have the users and groups defined, run lab-add-users on server X.  
  
Graduate students need a collaborative directory titled /opt/research,  
where they can store generated research results. Only members of the groups  
profs and grads should be able to create new files in the directory, and new  
files should have the following properties:  
• The directory should be owned by user root.  
• New files should be group owned by the group grads.  
• Professors (members of the group profs) should automatically have read/write access to new files.  
• Summer interns (members of the group interns) should automatically have read-only access to new files.  
• Other users (not a member of groups profs, grads, or interns) should not be able to access the directory and its contents at all.

**Questions 1 | CREATE LVM**  
Create the "LVM" with the name "source" by using 26PE's from the volume group "open". Consider the PE size as "8MB". Mount it on /mnt/secret with filesystem vfat.

First you need to see that volume group: open has Physical Extent set to 8MB:

# vgdisplay  
--- Volume group ---  
VG Name open  
System ID  
Format lvm2  
Metadata Areas 1  
Metadata Sequence No 5  
VG Access read/write  
VG Status resizable  
MAX LV 0  
Cur LV 0  
Open LV 0  
Max PV 0  
Cur PV 1  
Act PV 1  
VG Size 1016.00 MiB  
PE Size 8.00 MiB  
Total PE 127  
Alloc PE / Size 0 / 0  
Free PE / Size 127 / 1016.00 MiB  
VG UUID euwkrx-JMMc-yrDa-mc0s-QfNh-9wRb-ad2QA9

If PE Size is other than 8MB You should change it by typing:

vgchange -s 8M open

but before You do that, You need to remove all Logical Volumes from that group  
  
Next create LogicalVolume:

lvcreate -n source -l 28 open

Let's see if everything goes right:

lvdisplay open  
--- Logical volume ---  
LV Path /dev/open/source  
LV Name source  
VG Name open  
LV UUID t9aWn3-PxLl-CCNX-xXkG-Y6WI-bsbv-1e2Abw  
LV Write Access read/write  
LV Creation host, time dev.fivetag.pl, 2012-10-05 11:44:53 +0200  
LV Status available  
# open 0  
LV Size 224.00 MiB  
Current LE 28  
Segments 1  
Allocation inherit  
Read ahead sectors auto  
- currently set to 256  
Block device 253:2

Next, format as vfat:

mkfs -t vfat /dev/mapper/open-source

If not exist, create directory /mnt/secret

mkdir /mnt/secret

And mount it

mount /dev/mapper/open-source /mnt/secret

Question 2  
Create a group named "sysadmin"  
#groupadd -q 25000 sysadmin  
A user sarah and natasha should belongs to "manager" group as a secondary group  
# groupadd -q 25001 manager  
# useradd -G manager sarah;passwd sarah  
# useradd -G manager natasha;passwd natasha  
A user harry should not have access to interactive shell and he should not be a member of "manager" group  
useradd harry;passwd harry  
#vi /etc/passwd. Look for harry and change "/bin/bash" to "/sbin/nologin".  
save and exit.

**Questions 3 | DIRECTORY COLLABORATION:**  
Create the Directory "/home/manager" with the following characteristics. Group ownership of "/home/manager" should go to "manager" group. The directory should be have full permission for all members off "manager" group but not to any other users accept "root". Files created under "/home/manager" should get the same group ownership is set to the "manager" group.  
# mkdir /home/manager  
# chown nobody.manager /home/manager  
# chmod 2770 /home/manager

**Questions 4 | UPDATE THE KERNEL:**  
Install the appropriate Kernel from<ftp://instructor.example.com/ftp/updates>. Your machine should boot with updated kernel.  
there are two ways:  
first, we can get the related rpm from this ftp with wget for example:  
#wget ftp://[instructor.example.com/ftp/updates](ftp://instructor.example.com/ftp/updates)/kernel-2.6.32-XX.el6.x86\_64.rpm  
then we can install it:  
#rpm -ivh kernel-2.6.32-XX.el6.x86\_64.rpm  
The second and fastest way is using yum:  
#yum update kernel  
This option needs to set this ftp as a local repository, adding a .repo file in /etc/yum.repos.d/

**Questions 5 | CRON JOB:**  
The user sarah must configure a cron job that runs today at 14:23 today. and executes "/bin/echo "hyer" and deny the user max for creating cronjob .  
Since the job is specific and not periodically, we will use the command at:  
#at 1423  
>/bin/echo "hyer"  
>EOT  
to deny max use cronjob we need tu include him in /etc/cron.deny and /etc/at.deny

**Questions 6 | RESIZE LVM:**  
Resize the lvm "/dev/vgsrv/home" (/dev/myvol/vo) so that after reboot size should be in between 90MB to 120MB..

[root@rhel01 ~]# lvs  
LV VG Attr LSize Pool Origin Data% Move Log Copy% Convert  
lv\_root VolGroup -wi-ao-- 18.51g  
lv\_swap VolGroup -wi-ao-- 1.00g  
source open -wi-ao-- 800.00m  
home vgsrv -wi-a--- 200.00m  
[root@rhel01 ~]# lvresize /dev/vgsrv/home -L 120M  
WARNING: Reducing active logical volume to 120.00 MiB  
THIS MAY DESTROY YOUR DATA (filesystem etc.)  
Do you really want to reduce home? [y/n]: y  
Reducing logical volume home to 120.00 MiB  
Logical volume home successfully resized  
[root@rhel01 ~]# lvs  
LV VG Attr LSize Pool Origin Data% Move Log Copy% Convert  
lv\_root VolGroup -wi-ao-- 18.51g  
lv\_swap VolGroup -wi-ao-- 1.00g  
source open -wi-ao-- 800.00m  
home vgsrv -wi-a--- 120.00m

If you want to rename it

[root@rhel01 ~]# vgrename /dev/vgsrv  /dev/myvol  
  Volume group "vgsrv" successfully renamed to "myvol"  
[root@rhel01 ~]# lvrename /dev/myvol/home /dev/myvol/vo  
  Renamed "home" to "vo" in volume group "myvol"

**Questions 7 |   BIND THE "LDAP" FOR USER AUTHENTICATION:**  
Note the following. BASE DN: dc=example,dc=com ldap path ldap://instructor.example.com/ Download the certificate from "<ftp://instructor.example.com/pub/EXAMPLE-CA-CERT>" ldapuserX should login into your system . Where "X" is your system no.

**Questions 10 | ACCESS CONTROL LIST:**  
Copy the file /etc/fstab to /var/tmp and configure the "ACL" as mention following. The file /var/tmp/fstab is owned by the "root". The file /var/tmp/fstab belongs to the group "root" The file /var/tmp/fstab should not be executable by other's. The user "sarah" should able to read and write to the file. The user "natasha" can neither read nor write to the file. other users (future and current) shuold be able to read /var/tmp/fstab. Create a directory /data ,set default group as ftp so that when content will be created under this dir group ftp will be inherited.  
  
This can be done like this:  
  
cp /etc/fstab /var/tmp/  
chown root:root /var/tmp/fstab  
#mount -o remount,acl /var  
  
#chmod o-x /var/ftp/fstab  
#setfacl -m u:sarah:rw /var/ftp/fstab  
#setfal -m u:natasha:--- /var/ftp/fstab  
#setfacl -m o:r-- /var/ftp/fstabb  
#mkdir /data  
#chown root:ftp /data  
#chmod g+s /data  
  
Any input on this would be appreciated....

Here is the solution for the repository:  
  
[root@station]# vim /etc/yum.repos.d/**max.repo**  (Inside the directory /etc/yum.repos.d/ create a file with any name but the extension should be **.repo** which stands for repository linker file)  
Inside the file **max.repo** type in the following information:  
[Server]  
name=redhat  
baseurl=[ftp://redhat.domain10.example.com/ftp/pub/updates/x86\_64**S**erver](ftp://redhat.domain10.example.com/ftp/pub/updates/x86_64Server)  
enabled=1  
gpgcheck=0  
  
Save & Quit the file (Use :wq)  
In the name field u can give any name; In the 1st line, u can give any word; In the 2nd line for the name filed, give a single word name. I dont know whether multiple words work or not. But in the 3rd line, u have to give the ftp path given for configuring the repository.  
  
[root@station]# yum repolist  
This command will show whether your repository has been configured correctly.  
  
After this u can use commands like:  
[root@station]# yum install –y samba\*  
  
So, no need to download rpm packages.... but type the ftp url/link very carefully.

Hey guys,  
  
What is your opinion in turning the NetworkManager off during the exam? Here is what I am planning to do in my exams.  
  
#chkconfig NetworkManager off  
#service NetworkManager stop  
  
and continue with the static configuration...

Q: The user **saara** must configure a cron job that runs daily at **15:25** local time and executes **/bin/echo hello**  
  
# rpm –q cronie    (it shows whether crond was installed or not)  
If its not installed  
# yum install cronie  
# service crond restart  
#chkconfig crond on  
  
# su – saara (username)  
# crontab –e  
25 15 \*   \*   \*   /bin/echo “hello”

**Questions 13 | ADD USERS:**  
Create the user "dax" with uid 4223.

useradd -u 4223  dax

2/  Create new logical volume names lvm1 with extend 100 from the volume group names vg1. Consider the PE size as "16MB". Mount it on /lvm1 with filesystem vfat.

2/  
Check available Physical Volumes:

[root@centos-srv /]# pvs  
PV               VG              Fmt Attr PSize PFree  
/dev/sda2 vg\_centossrv lvm2 a-- 14.51g   0  
/dev/sda3 vg\_centossrv lvm2 a-- 4.99g 1016.00m  
/dev/sdb                         lvm2 a-- 1.00g 1.00g  
/dev/sdc                         lvm2 a-- 3.00g 3.00g  
/dev/sdd                         lvm2 a-- 2.00g 2.00g

Create new Volume Group called vg1 with a PE size as 16MB:

[root@centos-srv /]# vgcreatevg1]-s 16m /dev/sdc  
Volume group "vg1" successfully created  
[root@centos-srv /]# vgdisplay vg1  
--- Volume group ---  
VG Name                  vg1  
System ID  
Format                   lvm2  
Metadata Areas   1  
Metadata Sequence No 1  
VG Access                        read/write  
VG Status                        resizable  
MAX LV                   0  
Cur LV                   0  
Open LV                  0  
Max PV                   0  
Cur PV                   1  
Act PV                   1  
VG Size                  2.98 GiB  
PE Size                  16.00 MiB  
Total PE                         191  
Alloc PE / Size  0 / 0  
Free PE / Size   191 / 2.98 GiB  
VG UUID                  mmh0zU-dE4L-riOe-3IYe-AHYt-eqmu-NfQ5ek

Then you have to create Logical Volume called lvm1 with the number of extents 100:

[root@centos-srv /]# lvcreate -n lvm1 -l 100 vg1  
Logical volume "lvm1" created  
[root@centos-srv /]# lvdisplay vg1/lvm1  
--- Logical volume ---  
LV Path                  /dev/vg1/lvm1  
LV Name                  lvm1  
VG Name                  vg1  
LV UUID                  3xKivp-qR1N-nWsX-0Ied-FOIQ-avFt-wFJpic  
LV Write Access  read/write  
LV Creation host, time centos-srv, 2012-12-01 13:35:11 +0100  
LV Status                        available  
# open                           0  
LV Size                  1.56 GiB  
Current LE                       100  
Segments                         1  
Allocation                       inherit  
Read ahead sectors       auto  
- currently set to       1024  
Block device             253:2

Next, create VFAT filesystem on the created lvm1 volume and mount it to /lvm1 directory:

[root@centos-srv /]# mkfs.vfat /dev/mapper/vg1-lvm1 && mkdir /lvm1 && mount /dev/mapper/vg1-lvm1 /lvm1  
mkfs.vfat 3.0.9 (31 Jan 2010)  
unable to get drive geometry, using default 255/63 <----- SKIP THIS WARNING

Finally, let's check it:

[root@centos-srv /]# mount |grep lvm1  
/dev/mapper/vg1-lvm1 on /lvm1 type vfat (rw)

Hi All,  
  
First of all, would like to thank this forum on helping me to pass my RHCSA :-)  
  
The "concept" of the questions are still the same (pls take note).  
  
Some tips:  
  
1.) I did turn off the network manager (this will mess up your name resolution, it did on my test)  
2.) I did turn off iptables  
3.) configure your network config correctly and your yum! if youre yum works you will save a lot of time!  
4.) i rebooted so many times,  
--> kernel update  
--> lvm configuration  
  
4.) dont forget to chkconfig service on  
5.) use the physical machine to do your test when it comes to httpd and vsftpd installation/configuration  
6.) study and dont rely on dumps (maybe 30%) at least get a good grasp of the concept.

**Q1.   Create the following users, groups and group memberships:**  
-   Create a group named **sysadmin**  
-   A user **saara**who belongs to **sysadmin** as a secondary group.  
-   A user **Natasha** who also belongs to **sysadmin** as a secondary group.  
-   A user **harry** who does not have access to an interactive shell on the system, and who is not a member of **sysadmin.**  
-   **Saara, Natasha** and **harry** should all have the password of **avaster.**

# Groupaddsysadmin

# Useraddsaara

# Useradd Natasha

# Useradd –s /sbin/nologin harry

# Passwd saara

# Passwd Natasha

# Passwd harry

# Usermod –G sysadmin saara

# Usermod –G sysadmin natasha

**Q2. Create a collaborative directory /shared/sysadmin with the following characteristics:**  
-   Group ownership of **/shared/sysadmin** is **sysadmin**.  
-   The directory should be readable, writable and accessible to members of sysadmin, but not to any other user.(It is understood that root has access to all files and directories on the system).  
-   Files created in **/shared/sysadmin** automatically have group ownership set to the sysadmin group.

# Mkdir -p /shared/sysadmin

# Chgrpsysadmin /shared/sysadmin

# Chmod g+s /shared/sysadmin

# Chmod g+rwx /shared/sysadmin

# Chmod o-rwx /shared/sysadmin

**Q3. Install the appropriate kernel update from** [**ftp://instructor.example.com/ftpupdates**](ftp://instructor.example.com/ftpupdates)**. Thefollowing must also be met:**  
-   The updated kernel is the default kernel when the system is rebooted.  
-   The original kernel remains available and bootable on the system.  
# uname –r  
# Wget [ftp://instructor.example.com/ftpupdates/kernel\*](ftp://instructor.example.com/ftpupdates/kernel*)

# Rpm –ivh kernel<TAB>

# Vim /etc/grub.conf

Check for default (0 or 1)

**Q4.   Enable IP forwarding.**  
vim /etc/sysctl.conf  
  net.ipv4.ip\_forward=1  
**:wq**  
  
#sysctl –p  
  
**Q5.** The user **saara** must configure a cron job that runs daily at **15:25** local time and executes  
-   **/bin/echo hello**.  
# rpm –q cronie    (it shows whether crond was installed or not)  
If its not installed  
# yum install cronie  
# service crond restart  
#chkconfig crond on  
# su – saara  
$ crontab –e  
25 15 \*   \*   \*   /bin/echo “hello”

* [Like This](http://certcollection.org/forum/index.php?app=core&module=global&section=reputation&do=add_rating&app_rate=forums&type=pid&type_id=613661&rating=1&secure_key=e85cbea64fd52cdd091040af14d3ac1c&post_return=613661)

**Q6.** Resize the LVM(200MB)so that it should be in between **400MB** to**450MB**.

  (or)  **130MB to 150MB**.

   For **Extending**:

# lvs

#  df –h /dev/vgname/lvname

  #  Lvextend –L +210M /dev/vgname/lvname

(or)

# Lvresize –L 420M /dev/vgname/lvname

# Resize2fs –P /dev/vgname/lvname

# df –h /dev/vgname/lvname

  # lvs (or) lvdisplay  
  
For **Shrinking**

# lvs

# df –h /dev/vgname/lvname

# umount /dev/vgname/lvname

# e2fsck –f  /dev/vgname/lvname

# Resize2fs /dev/vgname/lvname 150M

# Lvresize –L 150M /dev/vgname/lvname

# mount /dev/vgname/lvname

# df –h /dev/vgname/lvname

# Lvs (or) lvdisplay

**Q7.   Bind the LDAP for user authentication. Note the following:**  
-   Dc=station, dc=example,dc=com  
-   Ldap path **ldap://instructor.example.com/**  
-   Download the certificate from[**http://instructor.example.com/pub/EXAMPLE-CA-CERT**](http://instructor.example.com/pub/EXAMPLE-CA-CERT)  
-   **ldapuserx** should be able to log into your system, where x is your station number, but will not have a home directory until you have completed the **autofs** requirement.

# System-config-authentication

User account LDAP

Dc=station, dc=example,dc=com

**ldap://instructor.example.com/**

**tick use tls**

[**http://instructor.example.com/pub/EXAMPLE-CA-CERT**](http://instructor.example.com/pub/EXAMPLE-CA-CERT)

**authentication method   LDAP password**

**# getent passwd ldapuserx**

# **service sssd restart**

# **chkconfig sssd on**

====================================================  
  
**Q8. Configure autofs to auto mount the home directories of LDAP users. Note the following:**  
-   **instructor.example.com**(192.168.0.254) NFS-exports **/home/guests** to your system, where is x is your station ip.  
-   Ldapuserx’s home directory is  **instructor.example.com:/home/guests/ldapuserx**  
-   Ldapuserx’s home directory should be automounted locally beneath /home as **/home/ldapuserx.**  
-   Home directories must be writable by their users.  
-   While you are able to log in as any of the users ldapuser1 through ldapuser20, the only home directory that is accessible from your system is ldapuserx.

# Vim /etc/auto.master

/home/guests   /etc/auto.guests

# Vim /etc/auto.guests

LdapuserX -rw    **instructor.example.com:/home/guests/ldapuserX**

  # Service autofs reload

  # Su – ldapuserX

**Q9.** Copy the file **/etc/fstab** to /**var/tmp**. Configure the permissions of **/var/tmp/fstab** so that:  
-   The file /var/tmp/fstab is owned by the root user.  
-   The file /var/tmp/fstab belongs to the group root.  
-   The file /var/tmp/fstab should not be executable by anyone.  
-   The user saara is able to read and write /var/tmp/fstab.  
-   The user Natasha can neither write nor read /var/tmp/fstab.  
-   All other users (current and future) have the ability to read /var/tmp/fstab.  
  
# **Cp /etc/fstab   /var/tmp/fstab**  
# **Chown root /var/tmp/fstab**  
# **Chgrp root /var/tmp/fstab**  
# **Chmod 664    /var/tmp/fstab**  
# **Setfacl –m u:saara:rw- /var/tmp/fstab**  
# **Setfacl –m u:Natasha:--- /var/tmp/fstab**  
# **Setfacl –m o::r--   /var/tmp/fstab**  
  
================================================================================  
  
**Q10.** Configure your system so that it is an **NTP** client of **instructor.example.com**

#  System-config-date

Synchronize date and time over network

Add **instructor.example.com in NTP server**

**In advance speed up initial synchronize**

**Ok**

Can you please explain the question "**Q2. Create a collaborative directory /shared/sysadmin with the following characteristics:" as i am not clear with the answers.**

Create a directory names as  **/shared/sysadmin**  
  
**#mkdir -p /shared/sysadmin**  
  
This folder owner should sysadmin  
  
**#chgrp sysadmin /shared/sysadmin**  
  
Refer the accessible permissions. according to the qns user below permissions.  
  
**#chmod g+rwxs /shared/sysadmin**   (Here used sticky bit)  
  
for others users  
  
**#chmod o=--- /shared/sysadmin**

* [Like This](http://certcollection.org/forum/index.php?app=core&module=global&section=reputation&do=add_rating&app_rate=forums&type=pid&type_id=645400&rating=1&secure_key=e85cbea64fd52cdd091040af14d3ac1c&post_return=645400)
* [Quote](http://certcollection.org/forum/index.php?app=forums&module=post&section=post&do=reply_post&f=81&t=160798&qpid=645400)
* [MultiQuote](http://certcollection.org/forum/index.php?app=forums&module=post&section=post&do=reply_post&f=81&t=160798&qpid=645400)
* [Thanks](javascript:%20ajaxThanks(%20'645400'%20);)
* [Report](http://certcollection.org/forum/index.php?app=core&module=reports&rcom=post&tid=160798&pid=645400&st=)

**Questions 10 | ACCESS CONTROL LIST:**  
Copy the file /etc/fstab to /var/tmp and configure the "ACL" as mention following. The file /var/tmp/fstab is owned by the "root". The file /var/tmp/fstab belongs to the group "root" The file /var/tmp/fstab should not be executable by other's. The user "sarah" should able to read and write to the file. The user "natasha" can neither read nor write to the file. other users (future and current) shuold be able to read /var/tmp/fstab. Create a directory /data ,set default group as ftp so that when content will be created under this dir group ftp will be inherited.  
  
This can be done like this:  
  
cp /etc/fstab /var/tmp/  
chown root:root /var/tmp/fstab  
#mount -o remount,acl /var  
  
#chmod o-x /var/ftp/fstab  
#setfacl -m u:sarah:rw /var/ftp/fstab  
#setfal -m u:natasha:--- /var/ftp/fstab  
#setfacl -m o:r-- /var/ftp/fstabb  
#mkdir /data  
#chown root:ftp /data  
#chmod g+s /data

**1.Configure Selinux it should be in enforcing mode.**

#Setenforce 1

#Vim /etc/sysconfig/selinux

SELINUX=enforcing  
  # reboot  
   After restart just flush all iptables rules:  
  # iptables –F  
  # service iptables save  
  
=================================================================  
  
**2. Configure a FTP server and allow local user to login across reboots.**  
  #rpm-q vsftpd  
If  FTP service is not installed then:

#yum install -y vsftpd\*

#service vsftpd status

# service vsftpd start (if service is not started)

#getsebool –a | grep ftp

#setsebool –P ftp\_home\_dir **on**

**#** service vsftpd restart

#chkconfig --list vsftpd

If service is not “on”, then:

# chkconfig vsftpd on

=====================================================================

**3. Configure a FTP server and allow local user to login across reboots and only your network gets access and anonymous download should be enabled.**  
   #rpm-q vsftpd  
If  FTP service is not installed then:  
  
  #yum install -y vsftpd\*

# service vsftpd status

# service vsftpd start (if service is not started)

# getsebool –a | grep ftp

# setsebool –P ftp\_home\_dir **on**

# service iptables start

# iptables –t filter –A INPUT ! –s **172.31.120.0/255.255.255.0** –p tcp --dport 21 –j REJECT

# service iptables save

# chkconfig --list iptables

# chkconfig iptables on (if service runlevel is not on)

# yum install –y ftp\*

**#** service vsftpd restart

# chkconfig --list vsftpd

# chkconfig vsftpd on (if service runlevel is not on)

In Base Machine:

# ftp **172.31.120.40**

# name: anonymous

   Password: <no password, just press Enter>

ftp>cd pub

ftp> ls (check if file is present; note FileName)

ftp> logout

# cd /var/ftp/pub  
# get <FileName>  (Download File to check)  
  
===================================================================  
  
  
**4. Configure a FTP server and allow local user to login across reboots and only your network gets access and anonymous download**&**upload should be enabled.**  
  #rpm-q vsftpd  
If  FTP service is not installed then:

  #yum install -y vsftpd\*

# service vsftpd status

# service vsftpd start (if service is not started)

# getsebool –a | grep ftp

# setsebool –P ftp\_home\_dir **on**

# setsebool –P allow\_ftpd\_anon\_write **on**

# vim /etc/vsftpd/vsftpd.conf

**anon\_upload\_enable = YES**  (Line 27: Uncomment)

  :wq

# chcon –Rt public\_content\_rw\_t /var/ftp/pub

# chgrp ftp /var/ftp/pub

# chmod 777 /var/ftp/pub

# service iptables start

# iptables –t filter –A INPUT ! –s **172.31.120.0/255.255.255.0** –p tcp --dport 21 –j REJECT

# service iptables save

# chkconfig --list iptables

# chkconfig iptables on (if service runlevel is not on)

# yum install –y ftp\*

**#** service vsftpd restart

# chkconfig --list vsftpd

# chkconfig vsftpd on (if service runlevel is not on)

In Base Machine:

# ftp 172.31.120.40

# name: **anonymous**

   Password: <no password, just press Enter>

ftp>cd pub

ftp> ls (check if file is present; note FileName)

ftp> logout

  # cd /var/ftp/pub  
  # put <FileName>

**5. Implement a web server for the site** [**http://domain80.example.com**](http://domain120.example.com/)  
- Download [**ftp://instructor.example.com/ftpupdates/main.html**](ftp://instructor.example.com/ftpupdates/main.html)  
- Rename the downloaded file to **index.html.**  
- Copy the index.html to the Document Root of your web server.  
- Do not make any modifications to the content of **index.html**.  
  
# rpm –q httpd  
If httpd service is not installed  
#yum install –y http\*  
# service httpd status  
# service httpd start (If service is not started)  
# vim /etc/httpd/conf/httpd.conf  
<VirtualHost **172.31.120.40**:80>  
ServerName **station40.domain80.example.com**  
DocumentRoot /var/www/html  
**DirectoryIndex index.html**  
</VirtualHost>  
:wq  
  
#httpd -t  
# service httpd restart  
# chkconfig httpd on  
# wget  [**ftp://instructor.example.com/ftpupdates/main.html**](ftp://instructor.example.com/ftpupdates/main.html)  
**#** mv main.html index.html  
**#** cp index.html /var/www/html  
# elinks **station40.domain80.example.com**  
**Or**  
Open Firefox and in address bar give: http://**station40.domain80.example.com**  
  
=========================================================================  
  
**6. Implement a virtual host for the site** [**http://www.domain80.example.com**](http://www.domain80.example.com/)**, then perform the following steps:** Set the document root to /var/www/virtual. **Also ensure that the user Natasha is able to create content in /var/www/virtual.**

#vim /etc/httpd/conf/httpd.conf

  NameVirtualHost **172.31.120.40**:80

  <VirtualHost**172.31.120.40**:80>

  DocumentRoot /var/www/virtual

  ServerName [**www.domain80.example.com**](http://www.domain120.example.com/)

**DirectoryIndex index.html**

  </VirtualHost>

**:wq**

  #httpd -t  
  #mkdir /var/www/virtual  
#wget  [**ftp://instructor.example.com/ftpupdates/main.html**](ftp://instructor.example.com/ftpupdates/main.html)  
**#**mv main.html index.html  
# cp index.html /var/www/virtual  
#service httpd restart  
#chkconfig httpd on (à Check before turning on)  
**# setfacl –m u:natasha:rwx /var/www/virtual (**àuser Natasha is able to create content**)**  
  
# vim /etc/hosts  
172.31.120.40 [www.domain80.example.com](http://www.domain80.example.com)

**7. Extend a directory public for the existing virtualhost.**  
  
# mkdir  /var/www/virtual/public  
# vim /etc/httpd/conf/httpd.conf  
  
NameVirtualHost **172.31.120.40**:80  
<VirtualHost **172.31.120.40**:80>  
DocumentRoot /var/www/virtual  
ServerName **www.domain80.example.com**

**DirectoryIndex index.html**

<Directory /var/www/virtual/public>  
Order allow,deny  
Allow from **station40.domain80.example.com**  
</Directory>  
</VirtualHost>  
:wq  
  
#httpd –t  
# service httpd restart  
# wget [**ftp://instructor.example.com/ftpupdates/station.html**](ftp://instructor.example.com/ftpupdates/station.html)  
# mv station.html index.html  
# cp index.html /var/www/virtual/public  
  
====================================================================  
  
**8. Extend a directory public for the existing webserver.**  
# mkdir  /var/www/html/public  
# vim /etc/httpd/conf/httpd.conf  
  
NameVirtualHost **172.31.120.40**:80  
<VirtualHost **172.31.120.40**:80>  
DocumentRoot /var/www/html  
ServerName **station40.domain80.example.com**

**DirectoryIndex index.html**

<Directory /var/www/html/public>  
Order allow,deny  
Allow from **station40.domain80.example.com**  
</Directory>  
</VirtualHost>  
:wq  
  
# httpd –t  
# service httpd restart  
# wget [**ftp://instructor.example.com/ftpupdates/station.html**](ftp://instructor.example.com/ftpupdates/station.html)  
# mv station.html index.html  
# cp index.html /var/www/html/public

* [Like This](http://certcollection.org/forum/index.php?app=core&module=global&section=reputation&do=add_rating&app_rate=forums&type=pid&type_id=613669&rating=1&secure_key=e85cbea64fd52cdd091040af14d3ac1c&post_return=613669)

**9. The remote directory instructor.example.com:/var/ftp/pub should be mounted to /mnt/tmp on your local machine while rebooting the system.**  
  
#mkdir /mnt/tmp  
#vim /etc/fstab  
Instructor.example.com:/var/ftp/pub    /mnt/tmp   nfs    defaults 0 0  
:wq  
#mount –a  
#mount  
  
========================================================================================================================  
  
**10. Configure NFS and share a directory /data which can be accessible by your network only.**  
  
# rpm –qa | grep nfs  
If nfs is not installed:  
# yum install –y nfs\*  
# service nfs status  
# service nfs start  
# mkdir /data  
# vim /etc/exports  
**/data \*.domain80.example.com(rw,sync)**  
:wq  
# service nfs restart  
# chkconfig --list nfs  
# chkconfig nfs on (if runlevel is not on)  
  
Go to base machine:  
# showmount –e **172.31.120.40**  
It shows /data   **172.31.120.40**(rw,sync)  
**OR**  
# cd /net or cd **172.31.120.40**  
# ls  
It shows /data   **172.31.120.40**(rw,sync)

**11. Share the /common directory via SMB.**  
a. your smb server must be a member of the LLC workgroup  
b. the share’s name must be General.  
c. the shared directory must be available to example.com domain clients only.  
d. alice must have read access to the share, authenticating with the same password “password” if necessary.  
  
# yum install –y samba\*  
# service **smb** start  
# service **nmb** start  
# mkdir /common  
# chcon –Rt samba\_share\_t /common  
# vim /etc/samba/smb.conf  
Workgroup = LLC  
[General]à Share Name  
Comment = Redhat ----- anyname  
Path = /common  
hosts allow = **172.31.120.**  
Browseable = Yes  
Valid users = alice  
Read list = alice  
Writable = Yes  
# smbpasswd –a alice  
Passwd:password  
# service **smb** restart  
# service **nmb** restart  
# chkconfig smb on  
# chkconfig nmb on  
  
Go to Base Machine:  
# **findsmb**  
**# smbclient** –L //**172.31.120.40/**  
#smbclient //**172.31.120.40**/common–Ualice  
Smb: \> ls

* [Like This](http://certcollection.org/forum/index.php?app=core&module=global&section=reputation&do=add_rating&app_rate=forums&type=pid&type_id=613671&rating=1&secure_key=e85cbea64fd52cdd091040af14d3ac1c&post_return=613671)

**Q1: Configure your host name to be stationX.redhat.com**.:  
  
Answer:  
----------  
  
**Change the host name**  
  
Renaming a server is relatively easy in Red Hat. Normally we would reboot the machine after modifying /etc/sysconfig/network, but to save time on the exam use the hostname command to make the change permanent.  
Our virtual machine is currently named rhel01. In this example we will rename it to machine01. We need to modify /etc/systconfig/network, run the hostname command, and then to be thorough restart the system logging service and check /etc/hosts:  
# cat /etc/sysconfig/network  
NETWORKING=yes  
HOSTNAME=rhel01  
# cat /etc/sysconfig/network | sed 's/HOSTNAME=.\*$/HOSTNAME=machine01/' >/etc/sysconfig/network.new  
# mv /etc/sysconfig/network.new /etc/sysconfig/network  
mv: overwrite `/etc/sysconfig/network'? y  
# cat /etc/sysconfig/network  
NETWORKING=yes  
HOSTNAME=machine01  
# hostname machine01  
# hostname  
machine01  
# service rsyslog restart  
Shutting down system logger:                               [  OK  ]  
Starting system logger:                                    [  OK  ]  
We can see the name change happen in the log file /var/opt/log/messages:  
Mar 25 18:58:13 rhel01 kernel: Kernel logging (proc) stopped.  
Mar 25 18:58:13 rhel01 rsyslogd: [origin software="rsyslogd" swVersion="4.6.2" x-pid="1293" x-info="http://www.rsyslog.com"] exiting on signal 15.  
Mar 25 18:58:13 machine01 kernel: imklog 4.6.2, log source = /proc/kmsg started.  
Mar 25 18:58:13 machine01 rsyslogd: [origin software="rsyslogd" swVersion="4.6.2" x-pid="2193" x-info="http://www.rsyslog.com"] (re)start  
  
With the name of our server changed, we should also check the /etc/hosts file. Often times there is an entry mapping 127.0.0.1 to the host name.  
# cat /etc/hosts  
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4  
127.0.0.1   rhel01  
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6  
# cp /etc/hosts /etc/hosts.old  
# cat /etc/hosts | sed 's/rhel01/machine01/' >/etc/hosts.new  
# mv /etc/hosts.new /etc/hosts  
# cat /etc/hosts  
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4  
127.0.0.1   machine01  
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6  
By default the command prompt is set to include the host name. At this point it still displays the old name. Don’t panic. Log out and back in to see the new name:  
[root@rhel01 ~]#  
[root@rhel01 ~]# exit  
logout  
Connection to 192.168.1.207 closed.  
Jasper:~ chouseknecht$ ssh root@192.168.1.207  
root@192.168.1.207's password:  
Last login: Sun Mar 25 18:45:15 2012 from 192.168.1.203  
[root@machine01 ~]#  
[root@machine01 ~]#

* 1. [root@nfsroot Desktop]# fdisk /dev/sdb1  
     Command (m for help): n  
     Command action  
        e   extended  
        p   primary partition (1-4)  
     p  
     Partition number (1-4): 1  
     First cylinder (1-207, default 1):  
     Using default value 1  
     Last cylinder, +cylinders or +size{K,M,G} (1-207, default 207): +300M  
       
     Command (m for help): t  
     Selected partition 1  
     Hex code (type L to list codes): 8e  
     Changed system type of partition 1 to 8e (Linux LVM)  
       
     Command (m for help): w  
     The partition table has been altered!  
       
     [root@nfsroot Desktop]# pvcreate /dev/sdb1  
       Writing physical volume data to disk "/dev/sdb1"  
       Physical volume "/dev/sdb1" successfully created  
       
     [root@nfsroot Desktop]# vgcreate open -s 8M /dev/sdb1  
       Volume group "open" successfully created  
       
     [root@nfsroot Desktop]# lvcreate -l 26 -n source /dev/open  
       Logical volume "source" created  
       
     verify with  
     #lvdisplay source  
       
     [root@nfsroot Desktop]# mkdosfs -v -F 32 /dev/open/source  
       
     mkdosfs 3.0.9 (31 Jan 2010)  
     unable to get drive geometry, using default 255/63  
     /dev/open/source has 255 heads and 63 sectors per track,  
     logical sector size is 512,  
     using 0xf8 media descriptor, with 425984 sectors;  
     file system has 2 32-bit FATs and 1 sector per cluster.  
     FAT size is 3277 sectors, and provides 419398 clusters.  
     There are 32 reserved sectors.  
     Volume ID is e8ad472a, no volume label.  
       
     [root@nfsroot Desktop]# mount /dev/open/source /mnt/secret/
* 2.  
  [root@nfsroot Desktop]# groupadd sysadmin  
  [root@nfsroot Desktop]# useradd sarah  
  [root@nfsroot Desktop]# useradd natasha  
  [root@nfsroot Desktop]# groupadd manager  
  [root@nfsroot Desktop]# usermod -G manager sarah  
  [root@nfsroot Desktop]# usermod -G manager natasha  
  [root@nfsroot Desktop]# passwd sarah  
  New password:  
  BAD PASSWORD: it is based on a dictionary word  
  Retype new password:  
  passwd: all authentication tokens updated successfully.  
    
  [root@nfsroot Desktop]# passwd natasha  
  Changing password for user natasha.  
  New password:  
  BAD PASSWORD: it is based on a dictionary word  
  Retype new password:  
  passwd: all authentication tokens updated successfully.  
    
  [root@nfsroot Desktop]# useradd harry -s /sbin/nologin  
    
  [root@nfsroot Desktop]# passwd harry  
  Changing password for user harry.  
  New password:  
  BAD PASSWORD: it is based on a dictionary word  
  Retype new password:  
  passwd: all authentication tokens updated successfully.  
    
  [root@nfsroot Desktop]# tail /etc/group  
  tcpdump:x:72:  
  slocate:x:21:  
  user01:x:500:  
  user02:x:501:  
  u1:x:502:  
  sysadmin:x:503:  
  sarah:x:504:  
  natasha:x:505:  
  manager:x:506:sarah,natasha  
  harry:x:507:  
  [root@nfsroot Desktop]#
* Posted 06 July 2012 - 12:53 AM
* 3.  
  #mkdir /home/manager  
  #groupadd manager  
  #chgrp manager /home/manager  
  #chmod 2770 /home/manager  
    
  5.  
  #crontab -e  
  23 14 5 7 5 /bin/echo "hyer" (today's date: 5th july thursday)  
    
  #crontab -l  
    
  #vim /etc/crontab.deny  
  max  
  :wq  
  save & exit  
    
  11.  
  #yum install vsftpd  
  #service vsftpd start  
  #vim /etc/hosts.deny  
  VSFTPD:remote.test  
    
  :wq  
    
  13.  
  #useradd -u 4223 dax  
  #tail /etc/passwd  
    
  14.  
    
  create partition of 250MB size  
  #fdisk /dev/sda or any available  
  label as : 82 for linux swap  
  save & exit  
  #mkswap /dev/sda2  
  #swapon /dev/sda2  
  #swapon -s

**Questions 15 | LOCATE THE FILES:  
locate the files of owner "dax" and copy to the directory /root/found directory**  
  
**mkdir /root/found**  
  
**you can use UID or user name to find all files that owns by dax.**  
**you can get UID from passwd file, if the UID is 505 then**  
  
**you can use this command**  
  
**find / -uid 505 –exec cp –r {} /root/found \;**  
  
**or**  
  
**find / -user dax -exec cp -r {} /root/found \;**  
  
**you must find all files because as you know every user have a directory in /var/spool/mail/$user, and the user nay be have emails and these are files owns by the user. So you will search from the main root “/”**  
  
**regrads**

All,  
I just completed the RH300 Rapid Track Coursework as well as both exams for the RHCSA and RHCE.  
  
Here are the questions and answers to what was presented to me. I do hope this helps with anyone who is trying to pass these exams. $400.00 US dollars per exam is a lot of money and as such, anything to assist people without having to continue to spend such large amounts of money makes it all worth it.  
  
Good luck to everyone.  
  
Keep up the great work with having this site be online and the information current.  
  
**RHCSA**  
**1. Reset the root password**  
Reboot the virtual server.  
Spacebar then select e to edit the primary vmlinuz entry.  
Select a to append at the end of the line then s for single the b to boot  
Now sitting at single user prompt  
# passwd (enter new password)  
# reboot or # init 5  
  
**2. Make the network static**  
#vim /etc/sysconfig/network-scripts  
BOOTPROTO=static  
IPADDR=x.x.x.x  
PREFIX=24  
or  
NETMASK=255.255.255.0  
GATEWAY=x.x.x.x  
or  
# vim /etc/sysconfig/network  
GATEWAY=x.x.x.x  
service network restart  
chkconfig network on  
  
ping instructor.example.com  
  
**3. Point to an external yum repository**  
/etc/yum.repos.d/examrepo.repo  
[exam-repo]  
name=exam repo  
baseurl=http://instructor.example.com  
  
confirm by executing: yum repolist enabled  
  
**4. Download Kernel and Kernel-Firmware**  
Install the appropriate kernel update from <ftp://instructor.example.com/>pub.  
The following must also be met:  
-   The updated kernel is the default kernel when the system is rebooted.  
-   The original kernel remains available and bootable on the system.  
  
YUM  
# yum install –y kernel\* --nogpgcheck  
# vim /boot/grub/grub.conf  
   default=0  
  
The kernel version will be the same except it will have a -debug as part of the vmlinuz file. That is the only versioning difference I saw in the install.  
  
RPM  
# wget [ftp://instructor.example.com/pub/kernel\*](ftp://instructor.example.com/pub/kernel*)  
# rpm –ivh kernel<TAB>  
# vim /etc/grub.conf  
   default=0  
  
**5. Kernel Parameter**  
Enabel kernel parameter rsvslg=ax08 (hex value)  
#vim /etc/grub.conf  
At the end of the vmlinuz rhgb quiet parameter append this entry rsvslg=1  
  
It should reflect in /proc/cmdline after reboot.  
  
**6. LVM**   
**yum install system-config-lvm – lvm gui**  
**yum install gnome-disk-utility – fdisk gui**   
  
Resize the LVM 200MB so that it should be in between 400MB to 450MB or 130MB to 150MB, Change extents to 50 and 8 MG. It also needs to be formatted with the VFAT file system  
  
# yum install –y system-config-lvm –nogpgcheck  
# yum install –y gnome-disk-utility --nogpgcheck  
  
Execute system-config-lvm to set up the requirements listed above. This will save you a lot of time on the exam. This should be used for anything requiring lvm functionality.  
Execute palimpsest to set up partitioning via fdisk if required. This may not be needed for this task but you should install it anyways just in case.  
You can also use fdisk manually as well. Just make sure the label is of vfat and not ext4.  
  
**7. User Management**  
Create the following users, groups and group memberships:  
-   Create a group named sysadmin  
-   A user sara who belongs to sysadmin as a secondary group.  
-   A user harry who also belongs to sysadmin as a secondary group.  
-   A user natasha who does not have access to an interactive shell on the system, and who is not a member of sysadmin.  
-   sara, natasha and harry should all have the password of vuserpass.  
  
# groupadd sysadmin  
# useradd sara  
# useradd harry  
# useradd –s /sbin/nologin natasha  
# passwd sara  
# passwd harry  
# passwd natasha  
# usermod –G sysadmin sara  
# usermod –G sysadmin natasha  
  
# usermod –Ga manager, hr, helpdesk sara  (this will add sara to different group in one line)  
# cat /etc/group (confirm that each of these users have their own group and are part sysadmin  
  
Copy the file /etc/fstab to /var/tmp. Configure the permissions of /var/tmp/fstab so that:  
-   The file /var/tmp/fstab is owned by the root user.  
-   The file /var/tmp/fstab belong to the group root.  
-   The file /var/tmp/fstab should not be executable by anyone.  
-   The user sara is able to read and write /var/tmp/fstab.  
-   The user Natasha can neither write nor read /var/tmp/fstab.  
-   All other users (current and future) have the ability to read /var/tmp/fstab.  
  
# cp /etc/fstab /var/tmp/fstab  
# chown root:root /var/tmp/fstab  
# chmod 664 /var/tmp/fstab  
# setfacl –m u:sara:rw- /var/tmp/fstab  
# setfacl –m u:natasha:--- /var/tmp/fstab  
# setfacl –m o::r--   /var/tmp/fstab  
Note: Remember all users cannot execute including the sara and natasha.  
  
Create a collaborative directory /shared/sysadmin with the following characteristics:  
-   Group ownership of /shared/sysadmin is sysadmin.  
-   The directory should be readable, writable and accessible to members of sysadmin, but not to any other user.  
(It is understood that root has access to all files and directories on the system).  
-   Files created in /shared/sysadmin automatically have group ownership set to the sysadmin group.  
  
# mkdir -p /shared/sysadmin  
# chgrp sysadmin /shared/sysadmin  
# chmod g+s /shared/sysadmin  
# chmod g+rwx /shared/sysadmin  
# chmod o-rwx /shared/sysadmin  
  
**8. CRON**  
The user sara must configure a cron job that runs daily at 14:25 local time and executes   /bin/echo “hello”.  
  
# yum install –y cron\* --nogpgcheck  
# service crond start  
# chkconfig crond on  
# su – sara  
$ crontab –e  
25 14 \*   \*   \*   /bin/echo “hello”  
  
**9. LDAP**  
# chkconfig nscd off  
# service nscd stop  
# system-config-authentication or system-config-auth  
User account LDAP  
dc=station, dc=example, dc=com  
ldap://instructor.example.com/  
tick use tls  
<http://instructor.example.com/pub/EXAMPLE-CA-CERT>  
authentication method LDAP password  
  
Note: The method listed above should work without having to edit anything. However listed below are the other steps to make sure it has the correct connectivity.  
  
# vim /etc/nsswitch.conf  
   passwd: files sss  
   shadow: files sss  
   group:    files sss  
# vim /etc/sssd/sssd.conf  
   ldap\_uri= ldaps://instructor.example.com  
   ldaps://instructor.example.com  
   ldap\_search\_base = dc=station,dc=example,dc=com  
# service sssd restart  
# chkconfig sssd on  
# getent passwd ldapuserx  
  
**10.    NTP**  
You must sync your time to an external time source which is instructor.example.com  
# chkconfig ntp on  
# service ntp start  
Select Date and Time from the top of the gnome desktop  
Remove all three of the default time sources and assign just the one listed in the question.  
  
**11.    FTP**  
Configure FTP access from your system. Clients within the remote test should not have anonomyous FTP access to your system.  
Yes, notice, you must configure you network connection!  
# yum install –y  vsftpd --nogpgcheck  
# chkconfig vsftpd on  
# service vsftpd start  
# vim /etc/vsftpd.conf  
  
**12.    Web Server**  
Configure your system as "web server" for the site <http://serverX.example.com> .  
Download the web page from <ftp://instructor.example.com/updates/station.html>  
Rename the downloaded page as "index.html"  
Copy the "index.html" page to the "document root"  
Do not make any modifications to the content of index.html.  
  
# <ftp://instructor.example.com/updates/station.html> or # wget <http://instructor.example.com/updates/station.html>  
# mv station.html index.html  
# cp index.html /var/www/html  
# vim /etc/http/conf/httpd.conf  
NameVirtualHost XX:80   
<VirtualHost XX:80>  
DocumentRoot **/var/www/html/**  
ServerName **serverX.example.com**  
</VirtualHost>  
:wq!  
# vim /etc/hosts  
192.168.0.X serverX.example.com  
:wq!  
# yum install –y firefox –nogpgcheck  
Select firefox after installed from the top of the gnome desktop and point to server.example.com and it should display some unusual text.  
  
**13.    Physical Disks – SWAP**  
Create a new swap partition that is 450 MB.  
# palimpsest (execute everything through the gui)  
or  
# fdisk /dev/sda  
n(ew)  
p(rimary)  
3  
Enter  
+450M  
t(ype)  
3  
82 (Linux swap / Solaris)  
w(rite)  
# partprobe  
# reboot  
# mkswap /dev/sda3  
# blkid /dev/sda3  
/dev/sda3: UUID=”36fbc448-b969-4dcb-b940-acd084eae6bb” TYPE=”swap  
# vim /etc/fstab  
UUID=”36fbc448-b969-4dcb-b940-acd084eae6bb”  swap  swap defaults 0 0  
:wq!  
# swapon –s  
# swapon –a  
# swapon –s  
  
**14.    User Creation**  
Create user Betty with user id of 1250 and home directory betty  
# useradd –m /home/betty betty  
# vim /etc/passwd  
# betty uid = 1250  
# :wq  
  
**15.    Files owned by specific user**   
Please locate the files of owner "jenny" and copy to the directory /root/found directory  
find / -user jenny -exec cp -prf {} /dest\_folder/ \;  
or  
find / -user jenny >> /root/found  
  
**16.    Search for a word in a single file**  
List all lines which have string "ush" from "/usr/share/dict/words" file and copy the lines in /root/word.found.  
# grep ush /usr/share/dict/words >> /root/word.found  
  
**RHCE**  
**1. IP Packet Forward**  
# vim /etc/sysctl.conf  
net.ipv4.ip\_forward=1  
**#:wq**  
# sysctl –p  
  
**2. SELINUX**  
# yum install –y system-config-securitylevel\* --nogpgcheck  
  
Set Linux to enforcing mode  
# setenforce 1  
or  
# vim /etc/sysconfig/selinux  
SELINUX=enforcing  
# reboot –h now  
  
**3. ISCSI**  
Import an iscsi disk from the server <hostname.domainname> instructor.example.com.  
The iscsi disk must be mounted as /mnt/iscsi. This mount should be persistent across the reboot.  
  
man –k iscsi or iscsiadmin  
Copy two commands and paste them to the command line to mount  
#fdisk /dev/sdb1  
#mkfs.ext4 /dev/sdb1  
#mkdir /mnt/iscsi  
#mount /dev/sdb1 /mnt/iscsi  
# vim/etc/mtab  
copy /dev/sdb1 /mnt/iscsi   ext4   defaults,\_netdev   0 0 to /etc/fstab  
  
or just create this line in /etc/fstab.  
  
Must make sure that \_netdev is in the mount entry for it to be recognized as an external device.  
  
**4. CRON**   
The user jean should not be able to add a cron job for herself.  
Add the entry for user jean to /etc/cron.deny.  
  
The crond daemon should be installed. If not you will need to execute:  
# yum install –y cronie –nogpgcheck  
# chkconfig crond on  
# service crond start  
  
# vim /etc/cron.deny  
jean  
:wq!  
  
# service crond restart  
Remove /etc/cron. allow otherwise do not put any names in there and the cron.deny file should take effect.  
  
**5. FTP – DropBox**  
# yum install –y vsftpd --nogpgcheck  
# chkconfig vsftpd on  
# service vsftpd start  
# mkdir /var/ftp/dropbox  
# chgrp ftp /var/ftp/dropbox  
# chmod 730 /var/ftp/dropbox  
# semanage fcontext –a –t public\_content\_rw\_t ‘/var/ftp/dropbox(/.\*)?’  
# setsebool –P allow\_ftp\_anon\_write on  
  
# vim /etc/vsftp/vsftpd.conf  
anon\_upload\_enable=yes  
chown\_upload=yes  
chown\_usernane=daemon  
anon\_umask=077  
  
# service vsftp restart  
#ip /etc/sysconfig/iptables-config  
IPTABLES\_MODULES=”nf\_conntrack\_ftp nf\_nat\_ftp”  
#iptables –A INPUT –m state –state ESTABLISHED,RELATED –j ACCEPT  
#iptables –A INPUT –p tcp –dport 21 –j ACCEPT  
#service iptables save  
  
**6. Postfix**  
Configure an SMTP mail server. Your host should be able to receive remote mails.  
Mail od <users> should be spooled to /var/spool/mail/<user>  
  
# yum install –y postfix\* --nogpgcheck  
# vim /etc/postfix/main.cf  
line 75 - myhostname = station.domainX.example.com  
line 83 - mydomain = domainX.example.com  
line 113  remove # inet\_interfaces = all   ( allow mail from all host)  
line 116 “ give # inet\_interfaces = localhost ( i will disable localhost only)  
# service postfix restart  
# chkconfig postfix on  
  
Alias  
All mail sent to the admin user should be received by natasha  
  
# vim /etc/aliases  
admin: natasha  
:wq  
# newaliases  
  
**7. Samba**  
Create a folder that will be shared out as common for access to user winuser. You must make sure that udp ports 137/138 and tcp ports 139/445 are open for access. The user is coming from network 172.24.200.0/24 and is part of the Staff group. The user should be able to read as well as write to the share.  
  
# yum install -y samba –nogpgcheck  
# chkconfig smb on  
# sevice smb start  
# mkdir /common  >>>> THIS SHOULD BE CREATED ALREADY  
# useradd –s /sbin/nologin –G STAFF winuserX  
# system-config-firewall  
Check samba from the listing with the associated ports of 137/udp, 138/udp, 139/tcp, 445/tcp  
Confirm the entries within iptables by executing the following  
# iptables -L /etc/sysconfig/iptables  
–A INPUT –p udp --dport 137:138 –j ACCEPT  
–A INPUT –p tcp –dport 139 –j ACCEPT  
–A INPUT –p tcp –dport 445 –j ACCEPT  
  
# vim /etc/samba/smb.conf  
hosts allow= domainX.example.com or 172.24.200.  
workgroup=STAFF  
  
[common]  
path= /common  
browseable=yes  
read only= bi  
writable= yes  
read list=winuser  
:wq!  
  
# testparm  
# semanage fcontext –a –t public\_content\_t '/common(/.\*)?'  
# semanage fcontext –a –t  samba\_share\_t  '/common(/.\*)?'  
# restorecon -RFvv /common  
# smbpasswd -a winuserX  
New SMB password: samba  
Retype new SMB passwd: samba  
# service smb restart  
  
Test this connection from your base machine.  
# smbclient //192.168.0.X/common -U winuserX%samba  
smb: \> touch samba\_testfile  
smb: \> exit  
  
**8. NFS**   
Share a directory /nfsshare over a network accessible from serverX.example.com. The first network of domainX.example.com will have read and write capabilities. The second network of domain133.example.com will have read only capability. Make sure that it is only using nfs version 4  
Note: The question may ask to use only nfs version 4  
  
**serverX.example.com**  
# mkdir /nfsshare  
# chmod –R 755 /nfsshare  
# vim /etc/exports  
/nfsshare   domainX.example.com(rw) <<< No spaces between the domain and the parentheses  
/nfsshare   domain133.example.com(ro) <<< No spaces between the domain and the parentheses  
:wq!  
# vim /etc/sysconfig/nfs  
MOUNTD\_NFS\_V4=”yes”  
:wq!  
# exportfs –ra  
  
**9. AUTOMOUNT**  
The ldap user must have a home directory on desktopx.example.com that is shared out from server.example.com. The home directory is mounted on /home/guests. There are also other users that need to have access to their home directories from this particular desktop. The users should have the ability to read and write to their own directory but not anyone elses.  
Note: I am not sure if both of these entries within the auto.guests file are correct. The safe one would be using this entry: ***\*  -rw instructor.example.com:/home/guests/&***   
The question may also ask to use only nfs version 4. The entry will be vers=4  
  
# vim /etc/auto.master  
/home/guests   /etc/auto.guests  
# vim /etc/auto.guests  
ldapuserX  -rw instructor.example.com:/home/guests/ldapuserX  
\*  -rw instructor.example.com:/home/guests/&    
# service autofs reload  
# su – ldapuserX  
[ldapuserX@instructor.example.com~]$  
  
**10.    SSH**  
Configure SSH Server.  
This service must be accessible only over (domain.example.com) .example.com network.  
  
Configure SSH access as follows: –  
susan has remote SSH access to your machine from within example.com    
Clients within my133t.org should NOT have access to ssh on your system  
  
- Now, user susan should be able to login via ssh with default configuration (provided the user exists).  
- To block my133t.org network  
  
# vim hosts.deny  
**sshd:\*.my133t.org**  
:wq!  
  
# chkconfig sshd on  
# service sshd retart  
  
**11.    Web Server**  
Host a virtual website over <http://serverX.example.com> and <http://wwwX.example.com.> The web page to be hosted is shared from instructor.example.com/pub/web/www.html.  This page should be renamed index.html and not edited and placed in the document root of both servers. Place it into the document root of /var/www/html for serverX.example.com and /var/www/virtual for wwwX.example.com  
  
The name resolution is provided on the DNS server.  
  
# <ftp://instructor.example.com/pub/web/www.html>  
# mv www.html index.html  
# cp index.html /var/www/html  
# cp index.html /var/www/virtual  
# vim /etc/html/conf/html.conf  
  
  
NameVirtualHost XX:80   
<VirtualHost XX:80>  
DocumentRoot **/var/www/html/**  
ServerName **serverX.example.com**  
</VirtualHost>  
  
NameVirtualHost XX:80   
<VirtualHost XX:80>  
DocumentRoot **/var/www/virtual/**  
ServerName **wwwX.example.com**  
</VirtualHost>  
  
# semanage fcontext –a –t httpd\_sys\_content\_t ‘/var/www/virtual(/.\*)?’  
# restorecon –RFvv /var/www/virtual  
# service httpd restart  
  
**12.    Script**  
Create a script in bash /root/script.sh. It should check for several variables. If the word is one it will print two. If the word is two it will print one. And if neither is true, redirect output to standard error.  
  
#!/bin/bash  
if [ “$1” == “one” ]  
then  
echo “two”  
elif [ “$1” == “two” ]  
then  
echo “one”  
else  
echo “error” 1>&2  
fi  
:wq  
  
# chmod +x /root/program  
  
#./ script.sh one  
# two  
#./ script.sh two  
# one  
#./ script.sh three  
#  
  
**13.    Mount**  
Mount an iso file /root/boot.iso on /disk. This mount should be persistent across system restarts.  
  
# mkdir /data  
# mount –o loop /root/boot.iso /data  
# vim /etc/mtab  
copy /root/boot.iso /disk  iso9660  loop,ro  0 0  
paste /etc/fstab  
or  
# vim /etc/fstab  
/root/boot.iso /disk  iso9660  loop,ro  0 0

**Questions 10 | ACCESS CONTROL LIST:**  
Copy the file /etc/fstab to /var/tmp and configure the "ACL" as mention following. The file /var/tmp/fstab is owned by the "root". The file /var/tmp/fstab belongs to the group "root" The file /var/tmp/fstab should not be executable by other's. The user "sarah" should able to read and write to the file. The user "natasha" can neither read nor write to the file. other users (future and current) shuold be able to read /var/tmp/fstab. Create a directory /data ,set default group as ftp so that when content will be created under this dir group ftp will be inherited.  
  
This can be done like this:  
  
cp /etc/fstab /var/tmp/  
chown root:root /var/tmp/fstab  
#mount -o remount,acl /var  
  
#chmod o-x /var/ftp/fstab  
#setfacl -m u:sarah:rw /var/ftp/fstab  
#setfal -m u:natasha:--- /var/ftp/fstab  
#setfacl -m o:r-- /var/ftp/fstabb  
#mkdir /data  
#chown root:ftp /data  
#chmod g+s /data

Q: The user **saara** must configure a cron job that runs daily at **15:25** local time and executes **/bin/echo hello**  
  
# rpm –q cronie    (it shows whether crond was installed or not)  
If its not installed  
# yum install cronie  
# service crond restart  
#chkconfig crond on  
  
# su – saara (username)  
# crontab –e  
25 15 \*   \*   \*   /bin/echo “hello”

I think you have to use rpm -ivh kernel in the exam. If you are asked to use yum then install is the correct one so that you keep the already existing kernel.  
  
- I see at least two typos in your autofs settings. can you correct those and try it again.

/etc/auto.master  
/rusers/ldap20 auto.rusers ( should have been /etc/auto.rusers)  
  
/etc/auto.rusers  
\*   rw   /hosts.domain20.example.com:/rusers/ldap20/&    (should have been hosts.domain20.example.com)

Hope that helps,

* 1. wget the firmware ( you will be given the URL for you to download it)  
     2. wget the kernel  
     3. rpm -ivh firmware  
     4. rpm -ivh kernel and by default the new kernel will be the default. You don't have to change the order but worth checking the grub.conf file.  
       
     That is it!
* Actually, proper way to do it is to configure Yum repo and do "yum update kernel".

Hello all,  
  
I passed on friday my EX200 or RHCSA exam with 300 points.  
  
My study materials Michael Jang and VTC RHCSA videos,  but think this is a bit too much theory, I would prefer various RHCSA exam question/ blogs which can be found on the internet in the first place. those books like Michael Jang and VTC are time killers  
  
I wil try to put all text stuff that I used for study in the section share.  
  
Still there are several points which you must know to pass:  
  
1. Reset roots pwd  - single user mode  
  
2. Working with LVM  
  
3. Working with fdisk also recommend cfdisk, saved my a..s  
  
4. creating users, groups, acl, crontab  
  
5. Autofs, and ldap client  
  
6. Configure a custom repo f.e for http, install kernel,  - I found pretty good lynx for a guestion  
  
7. Install HTTPd, Vsftpd  
  
  
  
Kind regards

**Questions 1 | CREATE LVM**  
Create the "LVM" with the name "source" by using 26PE's from the volume group "open". Consider the PE size as "8MB". Mount it on /mnt/secret with filesystem vfat.

First you need to see that volume group: open has Physical Extent set to 8MB:

# vgdisplay  
--- Volume group ---  
VG Name open  
System ID  
Format lvm2  
Metadata Areas 1  
Metadata Sequence No 5  
VG Access read/write  
VG Status resizable  
MAX LV 0  
Cur LV 0  
Open LV 0  
Max PV 0  
Cur PV 1  
Act PV 1  
VG Size 1016.00 MiB  
PE Size 8.00 MiB  
Total PE 127  
Alloc PE / Size 0 / 0  
Free PE / Size 127 / 1016.00 MiB  
VG UUID euwkrx-JMMc-yrDa-mc0s-QfNh-9wRb-ad2QA9

If PE Size is other than 8MB You should change it by typing:

vgchange -s 8M open

but before You do that, You need to remove all Logical Volumes from that group  
  
Next create LogicalVolume:

lvcreate -n source -l 28 open

Let's see if everything goes right:

lvdisplay open  
--- Logical volume ---  
LV Path /dev/open/source  
LV Name source  
VG Name open  
LV UUID t9aWn3-PxLl-CCNX-xXkG-Y6WI-bsbv-1e2Abw  
LV Write Access read/write  
LV Creation host, time dev.fivetag.pl, 2012-10-05 11:44:53 +0200  
LV Status available  
# open 0  
LV Size 224.00 MiB  
Current LE 28  
Segments 1  
Allocation inherit  
Read ahead sectors auto  
- currently set to 256  
Block device 253:2

Next, format as vfat:

mkfs -t vfat /dev/mapper/open-source

If not exist, create directory /mnt/secret

mkdir /mnt/secret

And mount it

mount /dev/mapper/open-source /mnt/secret

Question 2  
Create a group named "sysadmin"  
#groupadd -q 25000 sysadmin  
A user sarah and natasha should belongs to "manager" group as a secondary group  
# groupadd -q 25001 manager  
# useradd -G manager sarah;passwd sarah  
# useradd -G manager natasha;passwd natasha  
A user harry should not have access to interactive shell and he should not be a member of "manager" group  
useradd harry;passwd harry  
#vi /etc/passwd. Look for harry and change "/bin/bash" to "/sbin/nologin".  
save and exit.

**Questions 3 | DIRECTORY COLLABORATION:**  
Create the Directory "/home/manager" with the following characteristics. Group ownership of "/home/manager" should go to "manager" group. The directory should be have full permission for all members off "manager" group but not to any other users accept "root". Files created under "/home/manager" should get the same group ownership is set to the "manager" group.  
# mkdir /home/manager  
# chown nobody.manager /home/manager  
# chmod 2770 /home/manager

**Questions 4 | UPDATE THE KERNEL:**  
Install the appropriate Kernel from<ftp://instructor.example.com/ftp/updates>. Your machine should boot with updated kernel.  
there are two ways:  
first, we can get the related rpm from this ftp with wget for example:  
#wget ftp://[instructor.example.com/ftp/updates](ftp://instructor.example.com/ftp/updates)/kernel-2.6.32-XX.el6.x86\_64.rpm  
then we can install it:  
#rpm -ivh kernel-2.6.32-XX.el6.x86\_64.rpm  
The second and fastest way is using yum:  
#yum update kernel  
This option needs to set this ftp as a local repository, adding a .repo file in /etc/yum.repos.d/

**Questions 5 | CRON JOB:**  
The user sarah must configure a cron job that runs today at 14:23 today. and executes "/bin/echo "hyer" and deny the user max for creating cronjob .  
Since the job is specific and not periodically, we will use the command at:  
#at 1423  
>/bin/echo "hyer"  
>EOT  
to deny max use cronjob we need tu include him in /etc/cron.deny and /etc/at.deny

**Questions 1 | CREATE LVM**  
Create the "LVM" with the name "source" by using 26PE's from the volume group "open". Consider the PE size as "8MB". Mount it on /mnt/secret with filesystem vfat.

[root@rhel01 ~]# pvcreate /dev/sdc  
  Writing physical volume data to disk "/dev/sdc"  
  Physical volume "/dev/sdc" successfully created  
  
  
root@rhel01 ~]# vgcreate  -s 8m open /dev/sdc  
  Volume group "open" successfully created  
[root@rhel01 ~]# vgs  
  VG       #PV #LV #SN Attr   VSize  VFree  
  VolGroup   1   2   0 wz--n- 19.51g    0  
  open     1   0   0 wz--n-  7.99g 7.99g  
[root@rhel01 ~]# vgdisplay open  
  --- Volume group ---  
  VG Name                          open  
  System ID                       
  Format                                lvm2  
  Metadata Areas                1  
  Metadata Sequence No  1  
  VG Access                      read/write  
  VG Status                      resizable  
  MAX LV                                0  
  Cur LV                                0  
  Open LV                          0  
  Max PV                                0  
  Cur PV                                1  
  Act PV                                1  
  VG Size                          7.99 GiB  
  PE Size                          8.00 MiB  
  Total PE                        1023  
  Alloc PE / Size          0 / 0    
  Free  PE / Size          1023 / 7.99 GiB  
  VG UUID                          QhlZRz-MAk1-5Y9y-UbYi-LaYS-41lF-KUEzeN  
  
  
lvm> lvcreate -L 8M -n source open  
  Logical volume "source" created  
lvm> lvs  
  LV      VG       Attr  LSize  Pool Origin Data%  Move Log Copy%  Convert  
  lv\_root VolGroup -wi-ao-- 18.51g                                                                                  
  lv\_swap VolGroup -wi-ao--  1.00g                                                                                  
  source  open   -wi-a---  8.00m  
  
  
[root@rhel01 ~]# mke2fs -t vfat /dev/open/source  
mke2fs 1.41.12 (17-May-2010)  
Filesystem label=  
OS type: Linux  
Block size=4096 (log=2)  
Fragment size=4096 (log=2)  
Stride=0 blocks, Stripe width=0 blocks  
51296 inodes, 204800 blocks  
10240 blocks (5.00%) reserved for the super user  
First data block=0  
Maximum filesystem blocks=209715200  
7 block groups  
32768 blocks per group, 32768 fragments per group  
7328 inodes per group  
Superblock backups stored on blocks:  
32768, 98304, 163840  
  
Writing inode tables: done                                                        
Writing superblocks and filesystem accounting information: done  
  
  
  
[root@rhel01 ~]# mount /dev/open/source /mnt/secret/

**Questions 2 | USER'S GROUPS AND PERMISSION:**  
Create a group named "sysadmin" A user sarah and natasha should belongs to "manager" group as a secondary group . A user harry should not have access to interactive shell and he should not be a member of "manager" group. passwd for all user created should be "password".

groupadd sysadmin  
groupadd manager  
  
useradd  -G manager sarah  
useradd -G natash

**Questions 13 | ADD USERS:**  
Create the user "dax" with uid 4223.

useradd -u 4223  dax

**Questions 6 | RESIZE LVM:**  
Resize the lvm "/dev/vgsrv/home" (/dev/myvol/vo) so that after reboot size should be in between 90MB to 120MB..

[root@rhel01 ~]# lvs  
LV VG Attr LSize Pool Origin Data% Move Log Copy% Convert  
lv\_root VolGroup -wi-ao-- 18.51g  
lv\_swap VolGroup -wi-ao-- 1.00g  
source open -wi-ao-- 800.00m  
home vgsrv -wi-a--- 200.00m  
[root@rhel01 ~]# lvresize /dev/vgsrv/home -L 120M  
WARNING: Reducing active logical volume to 120.00 MiB  
THIS MAY DESTROY YOUR DATA (filesystem etc.)  
Do you really want to reduce home? [y/n]: y  
Reducing logical volume home to 120.00 MiB  
Logical volume home successfully resized  
[root@rhel01 ~]# lvs  
LV VG Attr LSize Pool Origin Data% Move Log Copy% Convert  
lv\_root VolGroup -wi-ao-- 18.51g  
lv\_swap VolGroup -wi-ao-- 1.00g  
source open -wi-ao-- 800.00m  
home vgsrv -wi-a--- 120.00m

If you want to rename it

[root@rhel01 ~]# vgrename /dev/vgsrv  /dev/myvol  
  Volume group "vgsrv" successfully renamed to "myvol"  
[root@rhel01 ~]# lvrename /dev/myvol/home /dev/myvol/vo  
  Renamed "home" to "vo" in volume group "myvol"

**RHCSA**  
**1. Reset the root password**  
Reboot the virtual server.  
Spacebar then select e to edit the primary vmlinuz entry.  
Select a to append at the end of the line then s for single the b to boot  
Now sitting at single user prompt  
# passwd (enter new password)  
# reboot or # init 5  
  
**2. Make the network static**  
#vim /etc/sysconfig/network-scripts  
BOOTPROTO=static  
IPADDR=x.x.x.x  
PREFIX=24  
or  
NETMASK=255.255.255.0  
GATEWAY=x.x.x.x  
or  
# vim /etc/sysconfig/network  
GATEWAY=x.x.x.x  
service network restart  
chkconfig network on  
  
ping instructor.example.com  
  
**3. Point to an external yum repository**  
/etc/yum.repos.d/examrepo.repo  
[exam-repo]  
name=exam repo  
baseurl=http://instructor.example.com  
  
confirm by executing: yum repolist enabled  
  
**4. Download Kernel and Kernel-Firmware**  
Install the appropriate kernel update from <ftp://instructor.example.com/>pub.  
The following must also be met:  
-   The updated kernel is the default kernel when the system is rebooted.  
-   The original kernel remains available and bootable on the system.  
  
YUM  
# yum install –y kernel\* --nogpgcheck  
# vim /boot/grub/grub.conf  
   default=0  
  
The kernel version will be the same except it will have a -debug as part of the vmlinuz file. That is the only versioning difference I saw in the install.  
  
RPM  
# wget [ftp://instructor.example.com/pub/kernel\*](ftp://instructor.example.com/pub/kernel*)  
# rpm –ivh kernel<TAB>  
# vim /etc/grub.conf  
   default=0  
  
**5. Kernel Parameter**  
Enabel kernel parameter rsvslg=ax08 (hex value)  
#vim /etc/grub.conf  
At the end of the vmlinuz rhgb quiet parameter append this entry rsvslg=1  
  
It should reflect in /proc/cmdline after reboot.  
  
**6. LVM**   
**yum install system-config-lvm – lvm gui**  
**yum install gnome-disk-utility – fdisk gui**   
  
Resize the LVM 200MB so that it should be in between 400MB to 450MB or 130MB to 150MB, Change extents to 50 and 8 MG. It also needs to be formatted with the VFAT file system  
  
# yum install –y system-config-lvm –nogpgcheck  
# yum install –y gnome-disk-utility --nogpgcheck  
  
Execute system-config-lvm to set up the requirements listed above. This will save you a lot of time on the exam. This should be used for anything requiring lvm functionality.  
Execute palimpsest to set up partitioning via fdisk if required. This may not be needed for this task but you should install it anyways just in case.  
You can also use fdisk manually as well. Just make sure the label is of vfat and not ext4.  
  
**7. User Management**  
Create the following users, groups and group memberships:  
-   Create a group named sysadmin  
-   A user sara who belongs to sysadmin as a secondary group.  
-   A user harry who also belongs to sysadmin as a secondary group.  
-   A user natasha who does not have access to an interactive shell on the system, and who is not a member of sysadmin.  
-   sara, natasha and harry should all have the password of vuserpass.  
  
# groupadd sysadmin  
# useradd sara  
# useradd harry  
# useradd –s /sbin/nologin natasha  
# passwd sara  
# passwd harry  
# passwd natasha  
# usermod –G sysadmin sara  
# usermod –G sysadmin natasha  
  
# usermod –Ga manager, hr, helpdesk sara  (this will add sara to different group in one line)  
# cat /etc/group (confirm that each of these users have their own group and are part sysadmin  
  
Copy the file /etc/fstab to /var/tmp. Configure the permissions of /var/tmp/fstab so that:  
-   The file /var/tmp/fstab is owned by the root user.  
-   The file /var/tmp/fstab belong to the group root.  
-   The file /var/tmp/fstab should not be executable by anyone.  
-   The user sara is able to read and write /var/tmp/fstab.  
-   The user Natasha can neither write nor read /var/tmp/fstab.  
-   All other users (current and future) have the ability to read /var/tmp/fstab.  
  
# cp /etc/fstab /var/tmp/fstab  
# chown root:root /var/tmp/fstab  
# chmod 664 /var/tmp/fstab  
# setfacl –m u:sara:rw- /var/tmp/fstab  
# setfacl –m u:natasha:--- /var/tmp/fstab  
# setfacl –m o::r--   /var/tmp/fstab  
Note: Remember all users cannot execute including the sara and natasha.  
  
Create a collaborative directory /shared/sysadmin with the following characteristics:  
-   Group ownership of /shared/sysadmin is sysadmin.  
-   The directory should be readable, writable and accessible to members of sysadmin, but not to any other user.  
(It is understood that root has access to all files and directories on the system).  
-   Files created in /shared/sysadmin automatically have group ownership set to the sysadmin group.  
  
# mkdir -p /shared/sysadmin  
# chgrp sysadmin /shared/sysadmin  
# chmod g+s /shared/sysadmin  
# chmod g+rwx /shared/sysadmin  
# chmod o-rwx /shared/sysadmin  
  
**8. CRON**  
The user sara must configure a cron job that runs daily at 14:25 local time and executes   /bin/echo “hello”.  
  
# yum install –y cron\* --nogpgcheck  
# service crond start  
# chkconfig crond on  
# su – sara  
$ crontab –e  
25 14 \*   \*   \*   /bin/echo “hello”  
  
**9. LDAP**  
# chkconfig nscd off  
# service nscd stop  
# system-config-authentication or system-config-auth  
User account LDAP  
dc=station, dc=example, dc=com  
ldap://instructor.example.com/  
tick use tls  
<http://instructor.example.com/pub/EXAMPLE-CA-CERT>  
authentication method LDAP password  
  
Note: The method listed above should work without having to edit anything. However listed below are the other steps to make sure it has the correct connectivity.  
  
# vim /etc/nsswitch.conf  
   passwd: files sss  
   shadow: files sss  
   group:    files sss  
# vim /etc/sssd/sssd.conf  
   ldap\_uri= ldaps://instructor.example.com  
   ldaps://instructor.example.com  
   ldap\_search\_base = dc=station,dc=example,dc=com  
# service sssd restart  
# chkconfig sssd on  
# getent passwd ldapuserx  
  
**10.    NTP**  
You must sync your time to an external time source which is instructor.example.com  
# chkconfig ntp on  
# service ntp start  
Select Date and Time from the top of the gnome desktop  
Remove all three of the default time sources and assign just the one listed in the question.  
  
**11.    FTP**  
Configure FTP access from your system. Clients within the remote test should not have anonomyous FTP access to your system.  
Yes, notice, you must configure you network connection!  
# yum install –y  vsftpd --nogpgcheck  
# chkconfig vsftpd on  
# service vsftpd start  
# vim /etc/vsftpd.conf  
  
**12.    Web Server**  
Configure your system as "web server" for the site <http://serverX.example.com> .  
Download the web page from <ftp://instructor.example.com/updates/station.html>  
Rename the downloaded page as "index.html"  
Copy the "index.html" page to the "document root"  
Do not make any modifications to the content of index.html.  
  
# <ftp://instructor.example.com/updates/station.html> or # wget <http://instructor.example.com/updates/station.html>  
# mv station.html index.html  
# cp index.html /var/www/html  
# vim /etc/http/conf/httpd.conf  
NameVirtualHost XX:80   
<VirtualHost XX:80>  
DocumentRoot **/var/www/html/**  
ServerName **serverX.example.com**  
</VirtualHost>  
:wq!  
# vim /etc/hosts  
192.168.0.X serverX.example.com  
:wq!  
# yum install –y firefox –nogpgcheck  
Select firefox after installed from the top of the gnome desktop and point to server.example.com and it should display some unusual text.  
  
**13.    Physical Disks – SWAP**  
Create a new swap partition that is 450 MB.  
# palimpsest (execute everything through the gui)  
or  
# fdisk /dev/sda  
n(ew)  
p(rimary)  
3  
Enter  
+450M  
t(ype)  
3  
82 (Linux swap / Solaris)  
w(rite)  
# partprobe  
# reboot  
# mkswap /dev/sda3  
# blkid /dev/sda3  
/dev/sda3: UUID=”36fbc448-b969-4dcb-b940-acd084eae6bb” TYPE=”swap  
# vim /etc/fstab  
UUID=”36fbc448-b969-4dcb-b940-acd084eae6bb”  swap  swap defaults 0 0  
:wq!  
# swapon –s  
# swapon –a  
# swapon –s  
  
**14.    User Creation**  
Create user Betty with user id of 1250 and home directory betty  
# useradd –m /home/betty betty  
# vim /etc/passwd  
# betty uid = 1250  
# :wq  
  
**15.    Files owned by specific user**   
Please locate the files of owner "jenny" and copy to the directory /root/found directory  
find / -user jenny -exec cp -prf {} /dest\_folder/ \;  
or  
find / -user jenny >> /root/found  
  
**16.    Search for a word in a single file**  
List all lines which have string "ush" from "/usr/share/dict/words" file and copy the lines in /root/word.found.  
# grep ush /usr/share/dict/words >> /root/word.found  
  
**RHCE**  
**1. IP Packet Forward**  
# vim /etc/sysctl.conf  
net.ipv4.ip\_forward=1  
**#:wq**  
# sysctl –p  
  
**2. SELINUX**  
# yum install –y system-config-securitylevel\* --nogpgcheck  
  
Set Linux to enforcing mode  
# setenforce 1  
or  
# vim /etc/sysconfig/selinux  
SELINUX=enforcing  
# reboot –h now  
  
**3. ISCSI**  
Import an iscsi disk from the server <hostname.domainname> instructor.example.com.  
The iscsi disk must be mounted as /mnt/iscsi. This mount should be persistent across the reboot.  
  
man –k iscsi or iscsiadmin  
Copy two commands and paste them to the command line to mount  
#fdisk /dev/sdb1  
#mkfs.ext4 /dev/sdb1  
#mkdir /mnt/iscsi  
#mount /dev/sdb1 /mnt/iscsi  
# vim/etc/mtab  
copy /dev/sdb1 /mnt/iscsi   ext4   defaults,\_netdev   0 0 to /etc/fstab  
  
or just create this line in /etc/fstab.  
  
Must make sure that \_netdev is in the mount entry for it to be recognized as an external device.  
  
**4. CRON**   
The user jean should not be able to add a cron job for herself.  
Add the entry for user jean to /etc/cron.deny.  
  
The crond daemon should be installed. If not you will need to execute:  
# yum install –y cronie –nogpgcheck  
# chkconfig crond on  
# service crond start  
  
# vim /etc/cron.deny  
jean  
:wq!  
  
# service crond restart  
Remove /etc/cron. allow otherwise do not put any names in there and the cron.deny file should take effect.  
  
**5. FTP – DropBox**  
# yum install –y vsftpd --nogpgcheck  
# chkconfig vsftpd on  
# service vsftpd start  
# mkdir /var/ftp/dropbox  
# chgrp ftp /var/ftp/dropbox  
# chmod 730 /var/ftp/dropbox  
# semanage fcontext –a –t public\_content\_rw\_t ‘/var/ftp/dropbox(/.\*)?’  
# setsebool –P allow\_ftp\_anon\_write on  
  
# vim /etc/vsftp/vsftpd.conf  
anon\_upload\_enable=yes  
chown\_upload=yes  
chown\_usernane=daemon  
anon\_umask=077  
  
# service vsftp restart  
#ip /etc/sysconfig/iptables-config  
IPTABLES\_MODULES=”nf\_conntrack\_ftp nf\_nat\_ftp”  
#iptables –A INPUT –m state –state ESTABLISHED,RELATED –j ACCEPT  
#iptables –A INPUT –p tcp –dport 21 –j ACCEPT  
#service iptables save  
  
**6. Postfix**  
Configure an SMTP mail server. Your host should be able to receive remote mails.  
Mail od <users> should be spooled to /var/spool/mail/<user>  
  
# yum install –y postfix\* --nogpgcheck  
# vim /etc/postfix/main.cf  
line 75 - myhostname = station.domainX.example.com  
line 83 - mydomain = domainX.example.com  
line 113  remove # inet\_interfaces = all   ( allow mail from all host)  
line 116 “ give # inet\_interfaces = localhost ( i will disable localhost only)  
# service postfix restart  
# chkconfig postfix on  
  
Alias  
All mail sent to the admin user should be received by natasha  
  
# vim /etc/aliases  
admin: natasha  
:wq  
# newaliases  
  
**7. Samba**  
Create a folder that will be shared out as common for access to user winuser. You must make sure that udp ports 137/138 and tcp ports 139/445 are open for access. The user is coming from network 172.24.200.0/24 and is part of the Staff group. The user should be able to read as well as write to the share.  
  
# yum install -y samba –nogpgcheck  
# chkconfig smb on  
# sevice smb start  
# mkdir /common  >>>> THIS SHOULD BE CREATED ALREADY  
# useradd –s /sbin/nologin –G STAFF winuserX  
# system-config-firewall  
Check samba from the listing with the associated ports of 137/udp, 138/udp, 139/tcp, 445/tcp  
Confirm the entries within iptables by executing the following  
# iptables -L /etc/sysconfig/iptables  
–A INPUT –p udp --dport 137:138 –j ACCEPT  
–A INPUT –p tcp –dport 139 –j ACCEPT  
–A INPUT –p tcp –dport 445 –j ACCEPT  
  
# vim /etc/samba/smb.conf  
hosts allow= domainX.example.com or 172.24.200.  
workgroup=STAFF  
  
[common]  
path= /common  
browseable=yes  
read only= bi  
writable= yes  
read list=winuser  
:wq!  
  
# testparm  
# semanage fcontext –a –t public\_content\_t '/common(/.\*)?'  
# semanage fcontext –a –t  samba\_share\_t  '/common(/.\*)?'  
# restorecon -RFvv /common  
# smbpasswd -a winuserX  
New SMB password: samba  
Retype new SMB passwd: samba  
# service smb restart  
  
Test this connection from your base machine.  
# smbclient //192.168.0.X/common -U winuserX%samba  
smb: \> touch samba\_testfile  
smb: \> exit  
  
**8. NFS**   
Share a directory /nfsshare over a network accessible from serverX.example.com. The first network of domainX.example.com will have read and write capabilities. The second network of domain133.example.com will have read only capability. Make sure that it is only using nfs version 4  
Note: The question may ask to use only nfs version 4  
  
**serverX.example.com**  
# mkdir /nfsshare  
# chmod –R 755 /nfsshare  
# vim /etc/exports  
/nfsshare   domainX.example.com(rw) <<< No spaces between the domain and the parentheses  
/nfsshare   domain133.example.com(ro) <<< No spaces between the domain and the parentheses  
:wq!  
# vim /etc/sysconfig/nfs  
MOUNTD\_NFS\_V4=”yes”  
:wq!  
# exportfs –ra  
  
**9. AUTOMOUNT**  
The ldap user must have a home directory on desktopx.example.com that is shared out from server.example.com. The home directory is mounted on /home/guests. There are also other users that need to have access to their home directories from this particular desktop. The users should have the ability to read and write to their own directory but not anyone elses.  
Note: I am not sure if both of these entries within the auto.guests file are correct. The safe one would be using this entry: ***\*  -rw instructor.example.com:/home/guests/&***   
The question may also ask to use only nfs version 4. The entry will be vers=4  
  
# vim /etc/auto.master  
/home/guests   /etc/auto.guests  
# vim /etc/auto.guests  
ldapuserX  -rw instructor.example.com:/home/guests/ldapuserX  
\*  -rw instructor.example.com:/home/guests/&    
# service autofs reload  
# su – ldapuserX  
[ldapuserX@instructor.example.com~]$  
  
**10.    SSH**  
Configure SSH Server.  
This service must be accessible only over (domain.example.com) .example.com network.  
  
Configure SSH access as follows: –  
susan has remote SSH access to your machine from within example.com    
Clients within my133t.org should NOT have access to ssh on your system  
  
- Now, user susan should be able to login via ssh with default configuration (provided the user exists).  
- To block my133t.org network  
  
# vim hosts.deny  
**sshd:\*.my133t.org**  
:wq!  
  
# chkconfig sshd on  
# service sshd retart  
  
**11.    Web Server**  
Host a virtual website over <http://serverX.example.com> and <http://wwwX.example.com.> The web page to be hosted is shared from instructor.example.com/pub/web/www.html.  This page should be renamed index.html and not edited and placed in the document root of both servers. Place it into the document root of /var/www/html for serverX.example.com and /var/www/virtual for wwwX.example.com  
  
The name resolution is provided on the DNS server.  
  
# <ftp://instructor.example.com/pub/web/www.html>  
# mv www.html index.html  
# cp index.html /var/www/html  
# cp index.html /var/www/virtual  
# vim /etc/html/conf/html.conf  
  
  
NameVirtualHost XX:80   
<VirtualHost XX:80>  
DocumentRoot **/var/www/html/**  
ServerName **serverX.example.com**  
</VirtualHost>  
  
NameVirtualHost XX:80   
<VirtualHost XX:80>  
DocumentRoot **/var/www/virtual/**  
ServerName **wwwX.example.com**  
</VirtualHost>  
  
# semanage fcontext –a –t httpd\_sys\_content\_t ‘/var/www/virtual(/.\*)?’  
# restorecon –RFvv /var/www/virtual  
# service httpd restart  
  
**12.    Script**  
Create a script in bash /root/script.sh. It should check for several variables. If the word is one it will print two. If the word is two it will print one. And if neither is true, redirect output to standard error.  
  
#!/bin/bash  
if [ “$1” == “one” ]  
then  
echo “two”  
elif [ “$1” == “two” ]  
then  
echo “one”  
else  
echo “error” 1>&2  
fi  
:wq  
  
# chmod +x /root/program  
  
#./ script.sh one  
# two  
#./ script.sh two  
# one  
#./ script.sh three  
#  
  
**13.    Mount**  
Mount an iso file /root/boot.iso on /disk. This mount should be persistent across system restarts.  
  
# mkdir /data  
# mount –o loop /root/boot.iso /data  
# vim /etc/mtab  
copy /root/boot.iso /disk  iso9660  loop,ro  0 0  
paste /etc/fstab  
or  
# vim /etc/fstab  
/root/boot.iso /disk  iso9660  loop,ro  0 0