Practice Set RHCSA

I. Hard link:
Create hardlink to /etc/fstab in /backup

Ans: # mkdir /backup

ln /etc/backup /backup

ls /backup

II. Create user:
Create a user eric with user Id 3345
Password for the user should be hellowelcometotheworld
Create sudo user who doesn't prompt for password

Ans: # useradd -u 3345 eric

passwd eric

vim /etc/sudoers.d/eric

eric ALL = (ALL) NOPASSWD:ALL

su – eric

tail /etc/shadow (must be able to display)

sudo -i (must be able to login to root without prompting password)

III. Add user:
Create the following user.
Create a group "adminuser"
Create a user natasha who has "adminuser" as a supplementary group.
Create a user harry who also has "adminuser" as his supplementary group.
Create a user sara who does not have an interactive shell nor does belong to the group "adminuser".
All users should be set with a password flegtrac.

Ans: # groupadd adminuser

useradd -G adminuser natasha

useradd -G adminuser harry

useradd -s /sbin/nologin sara

passwd natasha

passwd harry

passwd sara

su - sara (must not be allowed to login as sara)

IV. Account expiry:
User eric's account should be expired after 60 days

Ans: # tail /etc/passwd (eric user must exist)

chage -l eric

date -d "+60 days" +%F (copy date)

chage -E paste date eric

chage -l eric

V. Password expiry:
User eric's password should expire after 80 days

Ans: # chage -l eric

chage -M 80 eric

chage -l eric

VI. Change password:
User eric must change password on first login

Ans: # chage -l eric

chage -d 0 eric

chage -l eric (password must be changed on first login)

VII. Create directory:
Create a directory /data/dir1/
The user natasha and harry should be able to collaboratively work on this directory.
The files and directories created within this directory should automatically belong to the group sysadmin.
All the members of the group should have read or write access.
All other users should not have any permissions.

Ans: # groupadd sysadmin

tail /etc/passwd (check user exist or not)

usermod -g sysadmin natasha

usermod -g sysadmin harry

mkdir /data/dir1 -p

chown :sysadmin /data/dir1 -R

chmod 3770 /data/dir1 -R

su - natasha

$ umask

$ vim .bashrc

Umask 007

$ exit

su - natasha

$ umask (must display 007)

$ touch /data/dir1/f1

$ ls -la /data/dir1 (file must have rw permission user: natasha and group:sysadmin)

Same procedure for harry user

VIII. Default file permission:
Adjust default file permission for specific user.

Ans: login to specific user

$ umask

$ vim .bashrc

umask 007

$ exit

Log back

$ umask (must display 007)

IX. Copy file: Copy the file /etc/fstab to /var/tmp/fstab
The file should belong to the user root and group root.
The user natasha should be able read and write on the file.
The user harry should neither read nor write on the file.
All other users should have read permission on the file.

Ans: # ls /etc/fstab

cp /etc/fstab /var/tmp/

getfacl /var/tmp/fstab

setfacl -m -u:natasha:rw /var/tmp/fstab

setfacl -m -u:harry:-- /var/tmp/fstab

getfacl /var/tmp/fstab

X. Modify the global login scripts. Normal users should have a umask setting that prevents others from viewing or modifying new files and directories

Ans: # ls /etc/bashrc

vim /etc/bashrc (copy required umask contents)

ls /etc/profile.d/

vim /etc/profile.d/user.sh

Paste and edit

useradd abc

su - abc

$ umask (will have configured umask)

XI. Configure sshd on serverb to prevent users logging in as root.

Ans: # ls /etc/ssh/sshd_config

vim /etc/ssh/sshd_config

PermitRootLogin yes (change it to no)

systemctl restart sshd

ssh root@server (must not allow to login)

XII. Configure sshd on serverb to allow users to authenticate using ssh keys only rather than the passwords

Ans: # ssh-keygen

ssh-copy-id user@server

ls /etc/ssh/sshd_config

vim /etc/ssh/sshd_config

PermitRootLogin yes (change it to no)

PublicKeyAuthentication yes (uncomment)

PassWordAuthentication yes (change it to no)

systemctl restart sshd

ssh root@server (must not allow to login)

ssh otheruser@server (prompt for password and must not allow)

ssh user @server (must allow)

XIII. Preserve system journal

Ans: # ls /etc/systemd/journald.conf

vim /etc/systemd/journald.conf

#Storage=auto (uncomment and change it to persistent)

systemctl restart system-journald.service

reboot

ls /var/log/journal (dir must exist)

XIV. Configure NTP:
Configure your machine to be a NTP client of classroom.example.com and an alias is set content.example.com

Ans: # vim /etc/chrony.conf

server classroom.example.com iburst

systemctl restart chronyd.conf

XV. Configure the network as follows:
The IP address of your system should be: 172.25.250.10
Subnet Mask: 255.255.255.0
Name server: 172.25.250.254
Gateway: 172.25.250.254

Ans: # nmcli connection show

nmcli connection add con-name "new" ifname eth0 type ethernet ipv4.method manual ipv4.address 172.25.250.10/24 ipv4.gateway 172.25.250.254 ipv4.dns 172.25.250.254

nmcli connection show

nmcli connection up "new"

nmcli connection show (new connection must be up

XVI. Add additional IP address: 10.1.2.1/24, the network should automatically connect after reboot

Ans: # nmcli connection show (note down connection name)

ls /etc/NetworkConnections/sysconfig/Wired_connection_1

vim/etc/NetworkConnections/sysconfig/Wired_connection_1

IPADDR1 = 10.1.2.1

PREFIX1 = 24

nmcli connection reload

nmcli connection up "Wired_connection_1"

ip addr (must display two ip address)

XVII. Configure the network as follows:
The IP address of your system should be: 172.25.250.10
Subnet Mask: 255.255.255.0
Name server: 172.25.250.254
Gateway: 172.25.250.254

Ans: # nmcli connection show (note down connection name)

nmcli connection modify " Wired_connection_1" ipv4.address 172.25.250.10/24 ipv4.gateway 172.25.250.254 ipv4.dns 172.25.250.254

nmcli connection reload

nmcli connection up "Wired_connection_1"

ip addr (must display new ip address)

XVIII. Set hostname:
Set host name of VM1: servera.lab.example.com
Set host name of VM2: serverb.lab.example.com

Ans # hostname

vim /etc/hostname

servera.lab.example.com

reboot

hostname

Repeat same procedure on another server

XIX. Configure YUM:

Configure your machine such that you are able to download exam software from http://content.example.com/rhel8.2/x86_64/dvd/AppStream

And http://content.example.com/rhel8.2/x86_64/dvd/BaseOS

Ans: # yum repolist

yum list all

ls /etc/yum.repos.d/

vim /etc/yum.repos.d/mypack.repo

[BaseOS]

baseurl= http://content.example.com/rhel8.2/x86_64/dvd/BaseOS

enabled=true

gpgchech=false

name=mypack_baseOS

[AppStream]

baseurl= http://content.example.com/rhel8.2/x86_64/dvd/AppStream

enabled=true

gpgchech=false

name=mypack_AppStream

yum repolist

yum list all

XX. Backup files:

Create an archive /root/new.tar.gz which stores the backup of /usr/local

Ans: # tar -czf /root/new.tar.gz /usr/local

```
# tar -tzf /root/new.tar.gz
```

XXI. Find files:

Find the files owned by era and copy it to /root/findfiles.

Ans:

```
# mkdir /root/findfiles
# find / -user era
# find / -user era -exec cp -aprv {} /root/findfiles \;
# ls /root/findfiles/
```

XXII. Search words:

Display the matched for the words "seismic" in the /usr/share/dict/words and save the output to a file /root/wordlist

Ans:

```
# grep "seismic" /usr/share/dict/words
# grep "seismic" /usr/share/dict/words >> /root/wordlist
# cat /root/wordlist
```

XXIII. Cron job:

Natasha must run a job "logger testing" every 2 minutes

Ans:

```
# tail /etc/passwd
# su - natasha
$ crontab -l
$ crontab -e
*/02 * * * * logger " logger testing"
$ crontab -l
$ exit
# cat /var/log/messages ( you must see message displayed )
```

XXIV. Download file from http://bastion.lab.example.com/test.txt to student user home directory.

Ans:

```
$ wget http://bastion.lab.example.com/test.txt
$ chmod +x test.txt ( if you are executing the file)
```

XXV. Systemd.tmpfiles to delete temporary files in student user home directory

Ans: # ls /etc/tmpfiles.d/

vim /etc/tmpfiles.d/volatile.conf

d /run/volatile 0700 root root 30s

ls /run/ (volatile dir does not exist)

system.tmpfiles --create /etc/tmpfiles.d/volatile.conf

ls /run/volatile (volatile dir exist)

touch /run/volatile/f1

ls /run/volatile

sleep 30s

system-tmpfiles --clean /etc/tmpfiles.d/volatile.conf

ls /run/volatile (f1 does not exist)

XXVI. Tuned:
System should have a recommended profile.
Set it as default profile.

Ans: # tuned-adm active

tuned-adm recommended (copy)

tuned-adm profile (paste recommended profile)

tuned-adm active

XXVII. Debug http:
Make sure web server is configured and running.
Web server should be accessible from remote PC.
Web server should publish from tcp port 82

Ans: # yum install httpd

systemctl enable --now httpd

systemctl status httpd

ls /var/www/html

echo " hello web" >> /var/www/html/index.html

curl http://servera

ls /etc/httpd/conf/httpd.conf

Port 80 (change to 82)

semanage port -l grep http (copy tcp port context)

semanage port -a -t paste -p tcp 82

systemctl restart httpd

semanage port -l | grep http (you must find port 82 added to tcp)

firewall-cmd --list-all

firewall-cmd --permanent --add-port=82/tcp

firewall-cmd --permanent --add-service=http

firewall-cmd --reload

firewall-cmd --list-all (you must find tcp 82 port)

curl http://servera:82

On another system

$ curl http://servera:82

XXVIII. Configure selinux issues of web server, port labelling.

Ans: # systemctl status httpd (failed)

systemctl enable --now httpd (failed to enable)

sealert -a /var/log/audit/audit.log

Display httpd port labelling context is not added

semanage port -l grep http (copy tcp port context)

semanage port -a -t paste -p tcp 82

systemctl restart httpd

semanage port -l | grep http (you must find port 82 added to tcp)

curl http://servera:82

XXIX. configure SELinux:

Configure SELinux mode of your system as enforcing.

Ans: # getenforce

vim /etc/selinux/conf

SELINUX=permissive (change it to enforcing)

reboot

getenforce

XXX. Standard partition:
Create a standard partition of 300M with vfat as the file system.
Above partition should be mounted on /mnt/partn

Ans: # lsblk --fs

parted /dev/vdb print

parted /dev/vdb mklabel gpt

parted /dev/vdb mkpart

File system: xfs

Start : 2048s

End: 301MB

parted /dev/vdb print

udevadm settle

mkdir /mnt/partn

mkfs.fat -F 32 /dev/vdb1

lsblk -o UUID /dev/vdb1 (copy UUID)

vim /etc/fstab

UUID=paste /mnt/partn vfat defaults 0 0

systemctl daemon-reload

mount /mnt/partn

lsblk --fs

df -hT

XXXI. Swap partition:
Create a swap partition of 512M on your system.

Ans: # parted /dev/vdb print

parted /dev/vdb mkpart

File system: linux-swap

Start: 301MB

End: 813 MB

udevadm settle

mkswap /dev/vdb2

lsblk --fs (copy UUID)

vim /etc/fstab

UUID=paste swap swap defaults 0 0

systemctl daemon-reload

swaon –all

swapon --show

XXXII. LVM Creation:

Create a logical volume of 50 extents where one extent having the size of 16MB.

The logical volume has the name of database and volume group have name datastore.

The logical volume should be mounted under /mnt/database with the file system ext3 and should be automatically available on reboot.

Ans: # parted /dev/vdb print

parted /dev/vdb mkpart

File system: xfs

Start: 813 MB

End: 1713 MB

parted /dev/vdb print

parted /dev/vdb set 3 lvm on

parted /dev/vdb print

udevadm settle

pvcreate /dev/vdb3

pvdisplay

vgcreate datastore -s 16MB /dev/vdb3

vgdisplay

lvcreate -n database -l 50 datastore

lvdisplay (copy path)

mkdir /mnt/database

mkfs -t ext3 paste path

lsblk -o UUID paste path (copy UUID)

vim /etc/fstab

UUID= paste /mnt/database ext3 defaults 0 0

systemctl daemon-reload

mount paste path

df -hT

XXXIII. LVRESIZE:

Resize the logical volume "pics" to 1500M which belong to the volume group "VG". Any size between 1400M to 1600M is permissible.

Ans: # df -hT (note down file system)

vgdispaly (check space exist or not –if not add pv)

parted /dev/vdb print

parted /dev/vdb mkpart

File system: xfs

Start: 1001MB

End: 2000MB

parted /dev/vdb print

parted /dev/vdb set 4 lvm on

parted /dev/vdb print

udevadm settle

pvcreate /dev/vdb4

pvdisplay

vgextend VG /dev/vdb4

vgdisplay

lvdisplay (copy path)

lvextend -L 1500M paste lv path

lvdisplay

resize2fs paste path (for ext4) / xfs_growfs paste mount point (for xfs)

df -hT

XXXIV. AUTOFS:

The home directory of user "remoteuserX" are shared via NFS.
The bastion.lab.example.com shares home directory of "remoteuserX" via NFS.
Mount /rhome/remoteuserX to your system
The "remoteuserX" home directory is at bastion.lab.example.com:/rhome.
The "remoteuserX" home directory should be automounted locally beneath /rhome/remoteuserX.
The home directories must be writtable by their users.
Password of "remoteuserX" is flagtrac.

Ans: # tail /etc/passwd

su - remoteuserX

$ ls

$ exit

yum install autofs

systemctl enable --now autofs

systemctl status autofs

ls /etc/auto.master.d/

vim /etc/auto.master.d/direct.autofs

/- /etc/auto.direct

vim /etc/auto.direct

/rhome/remoteuserX -rw,sync,fstype=nfs4 bastion.lab.example.com:/rhome

systemctl restart autofs

su – remoteuserX

$ ls

XXXV. Containers:

Create a container logserver from an image rsyslog from registry.redhat.io
Login to registry.redhat.io with the redhat.com account
Configure the container with system services by an existing user "Wallah"
Service name should be container.logserver and configure it to start automatically across reboot.

Configure you most journal to store all across reboot.
Copy all journal from /var/log/journal and all subdirectories to /home/Wallah/container_logserver.
Configure to automount /var/log/journal from logserver (container) to /home/Wallah/container_logserver when container start.

Ans: # ls /etc/systemd/journald.conf

vim /etc/systemd/journald.conf

#Storage=auto (uncomment and change it to persistent)

systemctl restart system-journald.service

reboot

ls /var/log/journal (dir must exist)

mkdir /home/Wallah/container_logserver

cp -aprv /etc/log/journal /home/Wallah/container_logserver/

chown Wallah:Wallah /home/Wallah/container_logerver/ -R

chmod 777 /home/Wallah/journal -R

yum install module container-tools

exit

$ ssh Wallah@servera

$ ls -la /home/Wallah/container_logserver (owner must be Wallah)

$ podman run -d --name

XXXVI. Select boot target/ systemd target:

Configure system to automatically boot into multi-user target and set it as default target.

Ans: # systemctl get-default

systemctl set-default specify.target

systemctl get-default

reboot

XXXV. **Reset Root password on serverb / node2**

Ans: directly open the node2 console

Press ctl + alt + del

Using arrow key select rescue mode of os and press e

Go to linux line, at the end of the line

rd.break console=tty1

press ctl + x

mount

mount -o remount,rw /sysroot

chroot /sysroot

passwd root

Passwd: redhat

Retype : redhat

touch /.autorelabel

exit

#exit

Login prompt appears, using new passwd now you can login

XXXVIII. Fix boot issues related to fstab entries / file mounts.

Ans: directly open the node2 console

Press ctl + alt + del

Using arrow key select rescue mode of os and press e

Go to linux line, at the end of the line

System.target=emergency.target console=tty1

press ctl + x

mount

mount -o remount,rw /

mount -a

Now problem in fstab will be displayed

vim /etc/fstab

Delete the corrupt entry

systemctl daemon-reload

mount -a

#reboot

Login prompt appears, now you can login back