Step1:How to chane the root password of your physical machine.

Step1- When the kernal names come Press e

Step2- Go to the line linux16

Step3- Go to the "rhgb quite" remove this word and

Step4-Append init=/bin/bash

Step5-press ctrl+x

#mount –o remount,rw /

#passwd

#touch /.autorelabel

#exec /sbin/init

How to chane the root password of your Virtual machine.

Step1- When the kernal names come Press e

Step2- Go to the end line linux16

Step3- write rd.break console=tty1

Step4-press ctrl+x

#mount –o remount,rw /sysroot

#chroot /sysroot

#passwd

#touch /.autorelabel

#exit

#exit

Step2:Network Connection Modification

#nmcli connection show

#nmcli connection add con-name static type Ethernet if-name eth0

#nmcli connection modify static ipv4.addresses "172.25.x.10/24 172.25.254.254" ipv4.dns "172.25.254.254" ipv4.method manual connection.autoconnect yes

#nmcli connection up static

#nmcli connection show - -act ive

#ping classroom.example.com

#vim /etc/hostname

Server1.example.com

Wq!

Q1.Increase your swap partition by 512MB. Both swap partition must be available. Your new swap space should be mounted at the booting time also.

Answer:

#fdisk –l

fdisk /dev/vdb

n- add new partition

p- primary partition

default:1(partition)

First Sector- Default Sector

Last Sector- +512M

t- Type

l- listing the hexa code

Hexa code- 82 (Swap Partition)

p- print the partition table

w- Save the changes

#partprobe –to update the partition table

#fdisk –l – to list the partition

#mkswap /dev/vdb1

#vim /etc/fstab

/dev/vdb1 swap swap defaults 0 0

Save and exit

#blkid-to display the block id of partition

swapon /dev/vdb1

#mount –a

#free –m

Q2.Create a volumegroup named as Oraclevg which having physical extent size of 8MB.

-> Create a logical volume red_lvl of 100 extents.

-> Assign ext3 filesystem for red_lvl. red_lvl should be avilable permanantly on /mnt/data directory.

#fdisk /dev/vdb

n- add new partition

p- primary partition

default:1(partition)

First Sector- Default Sector

Last Sector- Default Sector

t- Type

l- listing the hexa code

Hexa code- 8e (LVM Partition)

p- print the partition table

w- Save the changes

#partprobe

#pvcreate /dev/vdb2

#vgcreate -s 8M oraclevg /dev/vdb1

#lvcreate -n red_lvl -l 100 oraclevg ….(-l 100 extent size * 8M physical size = 800M original size of lvm)

#vgdisplay

#lvdisplay

#mkfs.ext3/ext4/vfat/xfs /dev/oraclevg/red_lvl

#mkdir /mnt/data

#vim /etc/fstab

/dev/oraclevg/red_lvl (or block id) /mnt/data ext3 defaults 0 0

Save and exit

#mount –a

#df –HT

Q3. Resize your logical volume "homeval" upto 250M without loosing any data.(After resizing lvm size will be accepted between the range of 245MB-255MB).

Note : First check the size of VG and LVM accordingly that decide whether you want to reduce or extend the lvm.

Following steps for lvm reduce:

umount /mnt/data

e2fsck –f /dev/homevg/homeval

resize2fs /dev/homevg/homeval 250M

lvreduce -L 250M /dev/homevg/homeval

mount –a

Following steps for lvm extend:

Note : check the size of VG to extend the LVM

resize2fs /dev/homevg/homeval 250M

lvextend -L 250M /dev/homevg/homeval

lvdisplay

Q4.Create the following users, group, group memberships

-> A group named sysadmins

->A user natasha who belongs to sysadmins as a secondary group.

-> A user harry who also belongs to sysadmins as a secondary group.

-> A user sarah who doesnot have access to an interactive shell on the system and who is also not member of sysadmins group.

-> natasha,harry and sarah should all have the password of "postroll".

#groupadd sysadmins

#useradd –G sysadmins natasha

#useradd –G sysadmins harry

#useradd –s /sbin/nologin sarah

#su - sarah

#echo "postroll" |passwd --stdin natasha

#echo "postroll" |passwd --stdin harry

#echo "postroll" |passwd --stdin sarah

Q5.Create collaborative directory /home/materials with the following characteristics:

-> Group ownership of /home/materials should be goes to sysadmins group.

-> The directory should be readable, writable and accessible to the member of sysadmins but not to any other users.

-> Files created in /home/materials automatically have group ownership set to the sysadmins group.

mkdir –p /home/materials

#chgrp sysadmins /home/materials

#ls –l /home/materials

#chmod 2770 /home/materials

cd /home/materials

#touch file{1..5}

ls –l (check the group ownership of file and directory)

Q6.The user natasha must configure a cron job that runs daily at 14:23 local time and executes /bin/echo "Hello_world".

#crontab –l

#su – Natasha

#crontab –l

#crontab –e

23 11 * * * /bin/echo Hello_world

Save and exit

#crontab –l

#exit from Natasha

#systemctl restart crond.service

#su – natasha

#mail

Q7. 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 natasha is able to read and write /var/tmp/fstab.

-> The user harry can neither write nor read /var/tmp/fstab.

-> All other users (current,future) have the ability to read /var/tmp/fstab.

#cp /etc/fstab /var/tmp

#ls –l /var/tmp/fstab

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

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

#getfacl

Q8.Configure your system so that it is an NTP client of classroom.example.com.

#date

#vim /etc/chrony.conf

Make the following changes

1.comment (#) on

server0.rhel.pool.ntp.org,iburst

server1.rhel.pool.ntp.org,iburst

server2.rhel.pool.ntp.org,iburst

2.Type the following line in end of the file

server classroom.example.com iburst

3.save and exit

#systemctl restart chronyd.service

#date

OR

#yum install system-config-date

#system-config-date

When the POP UP comes do the following steps

1.Delete the entry one by one

2. click on ADD button and write

classroom.example.com

3.click on empty space to initialize server

4.click Ok

#systemctl restart chronyd.service

Q9.Locate the files having ownership set to user harry and copy all those files to /root/resultdir/ directory.

#find / -user harry

#mkdir –p /root/resultdir

#find / -user harry –exec cp –av {} /root/resultdir/ \;

#cd /root/resultdir

#ls –a

Q10.Create a user jean having user identity as 4032 and his home directory should be in /India/Redhat directory.

#mkdir –P /India/Redhat

#useradd –u 4032 –d /India/Redhat jean

#su – jean

#pwd

#exit

#cat /etc/passwd

Q11.Search all the lines from /usr/share/dict/words which having word "fish" and store the output to the /root/flectrag file and arrange them in correct order.

#touch /root/flectrag

#grep fish /usr/share/dict/words > /root/flectrag

#cat /root/flectrag

Q13. Make a tarball of existing /home directory in .gz format and put that tarball in /root.

-> Create a bzip2 compression of /etc directory name of compression etc.tar.bz2 and put this file in /root directory.

du –sh /home

tar –cvjf /root/home.tar.gz /home

#du –sh /root/home.tar.gz

#du –sh /etc

tar –cvzf /root/etc.tar.bz2 /root

#du –sh /root/etc.tar.bz2

Q14.Selinux must be running in enforcing mode.

#getenforce

#vim /etc/sysconfig/selinux

Set here,

SELINUX = enforcing

:wq

#Reboot

#getenforce

#Reboot the system

Q15.Configure yum client side repository using following url http://classroom.example.com/content/rhel7.0/x86_64/dvd

#cd /etc/yum.repos.d

#ls

#vim redhat.repo

Add the following lines

[redhat]

gpgcheck = 0

enabled = 1

baseurl = http://classroom.example.com/content/rhel7.0/x86_64/dvd

name = welcome to linux

wq

#yum clean all

#yum repolist all

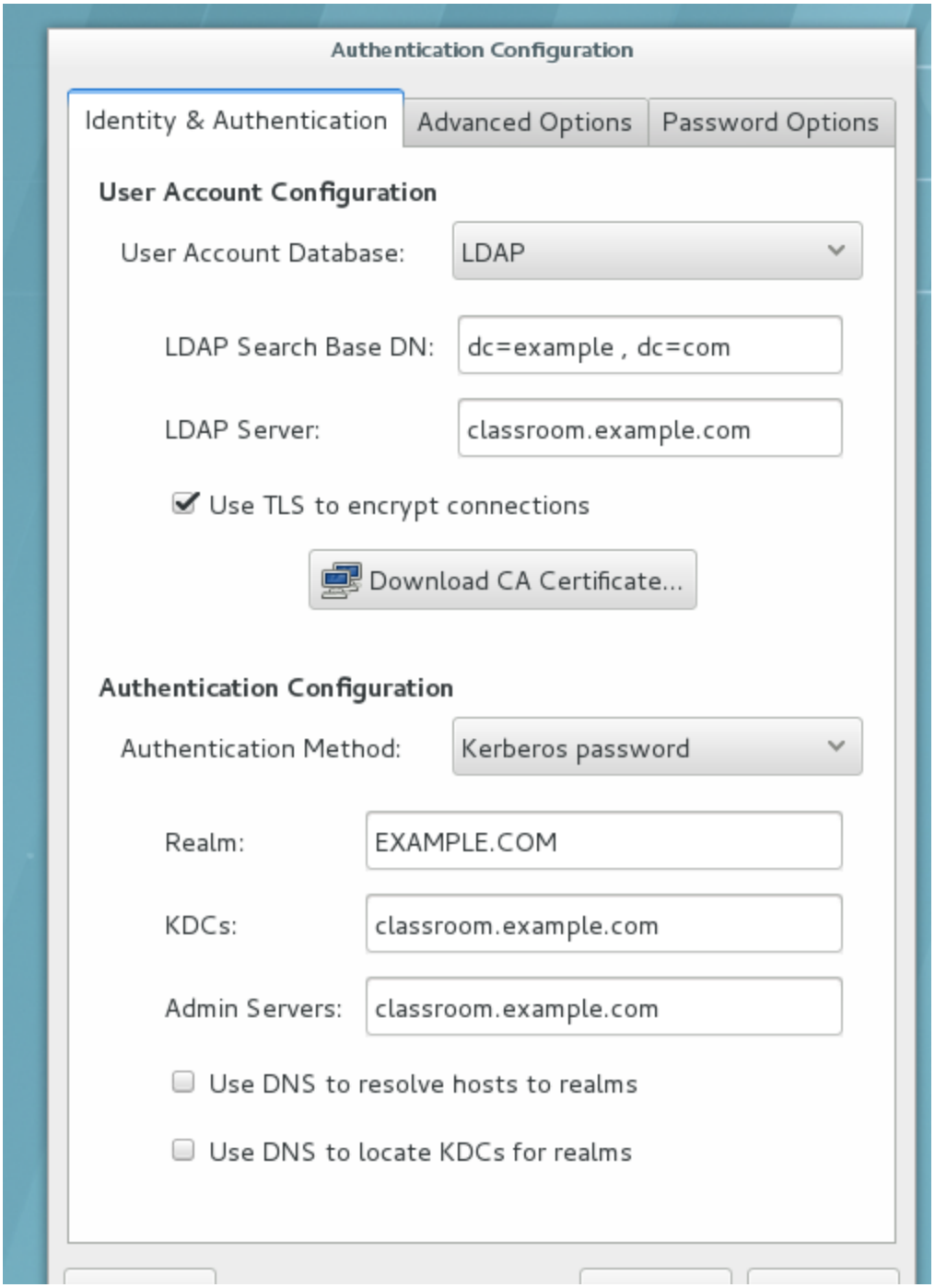
#yum update all

Q16.Install the appropriate kernel update from http://classroom.example.com/pub/updates.The following crieteria must also be meet: -> The updated kernel is the default kernel when the system is rebooted. -> The original kernel remains available and bootable on the system.

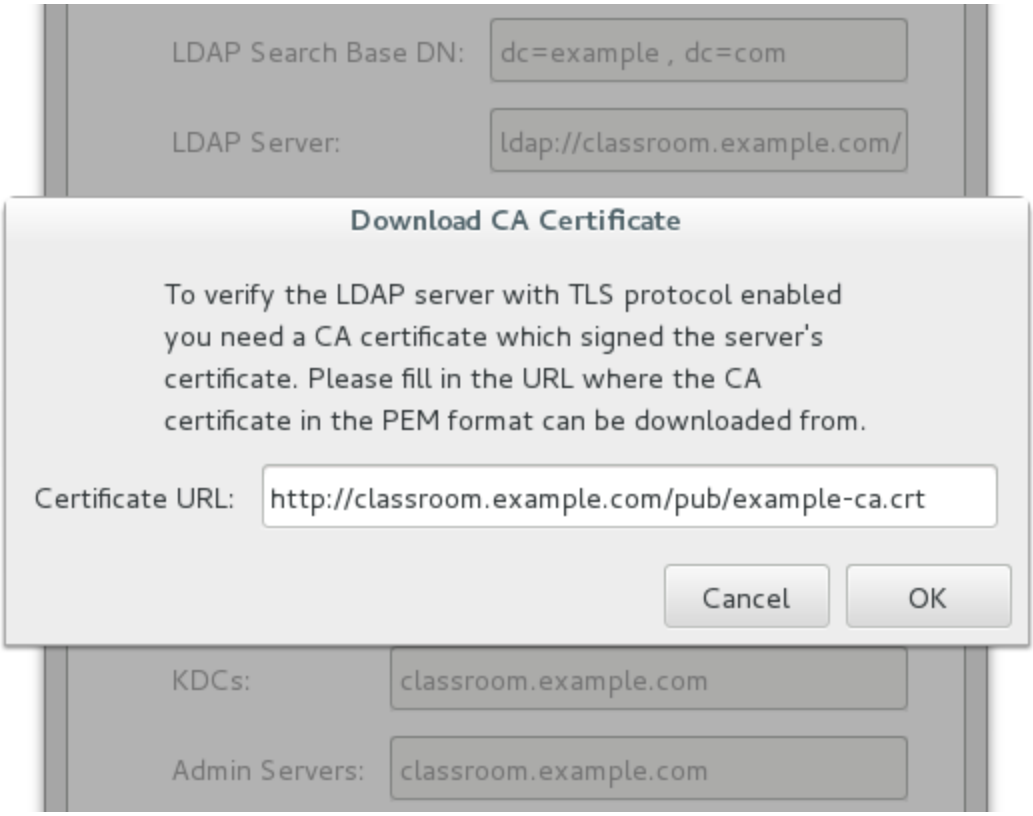
#cd /etc/yum.repos.d
#ls
#vim kernal.repo
Add the following lines
[kernel]
gpgcheck = 0
enabled = 1
baseurl = http://classroom.example.com/pub/updates/errata
name = welcome to linux
wq

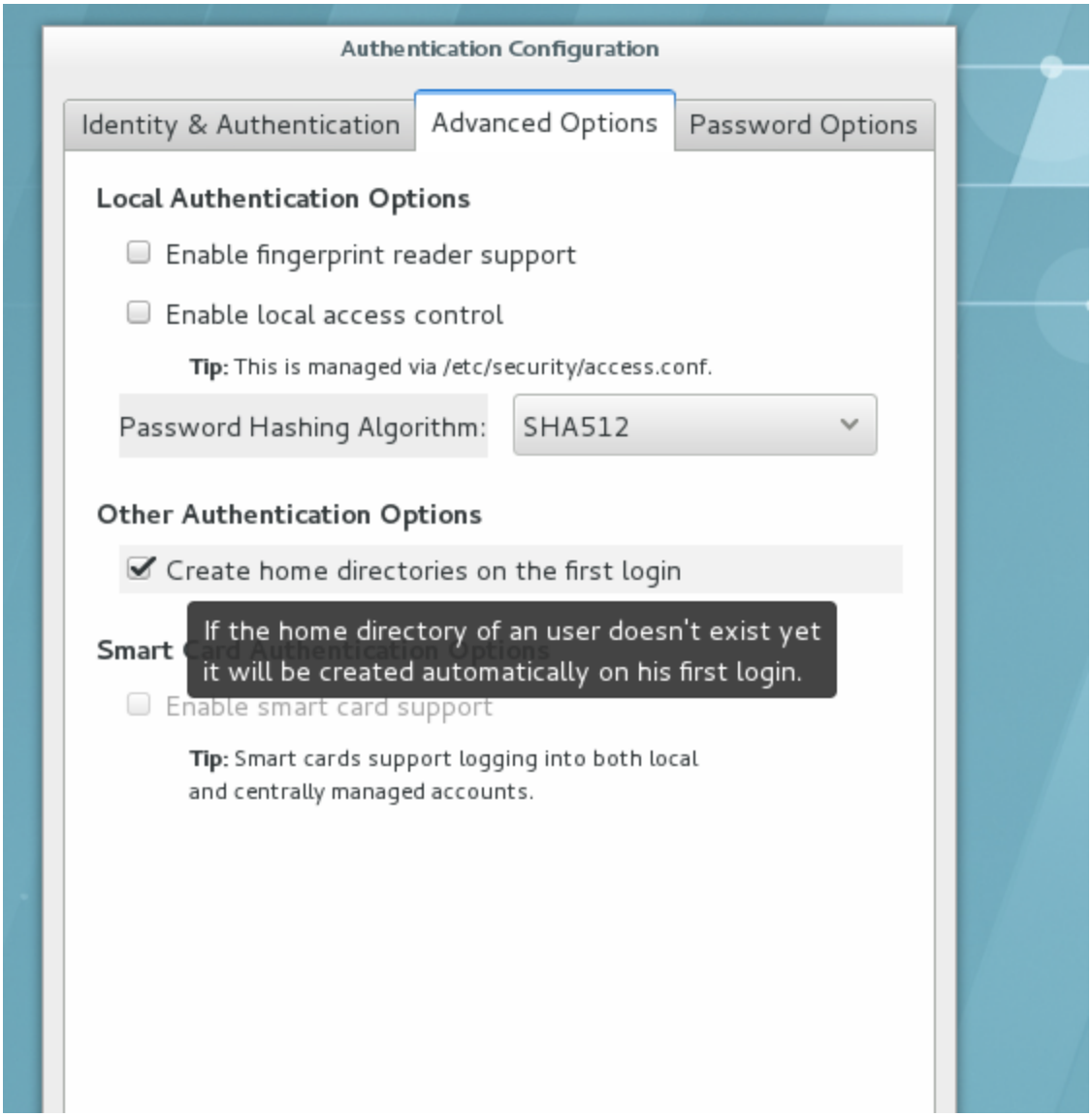
#yum clean all
#yum repolist all
#yum update all
Note: Reboot the system

Q17.Bind to the LDAP domain 'dc=example,dc=com' provided by classroom.example.com for user authentication. Note the following: -> ldapx should be able to log into your system, where x is your station number. but will not have a home directory untill you have completed the autofs requirement below. -> ldapx have a password of "redhat". -> you will get your CA certficate at http://classroom.example.com/pub/example-ca.crt
#yum install sssd* authconfig-gtk* krb5-workstation* -y
#system-config-authentication
When the prompt open please add the following:


Authentication Configuration
Identity & Authentication
Advanced Options
Password Options
User Account Configuration
User Account Database:
LDAP
LDAP Search Base DN:
dc=example , dc=com
LDAP Server:
classroom.example.com
Use TLS to encrypt connections
Download CA Certificate...
Authentication Configuration
Authentication Method:
Kerberos password
Realm:
EXAMPLE.COM
KDCs:
classroom.example.com
Admin Servers:
classroom.example.com
Use DNS to resolve hosts to realms
Use DNS to locate KDCs for realms

6_64


LDAP Search Base DN:
dc=example , dc=com
LDAP Server:
ldap://classroom.example.com/
Download CA Certificate
To verify the LDAP server with TLS protocol enabled you need a CA certificate which signed the server's certificate. Please fill in the URL where the CA certificate in the PEM format can be downloaded from.
Certificate URL:
http://classroom.example.com/pub/example-ca.crt
Cancel
OK
KDCs:
classroom.example.com
Admin Servers:
classroom.example.com



#getent passwd ldapuser1

Q18.Configure autofs to automount the home directories of LDAP users. Note the following: -> (172.25.254.254) NFS-exports /home/ to your system, where 'x' is your station number. -> ldapx's home directory is /home/guests. -> ldapx's home directory should be

locally name as /home/guests/ldapuserx. -> home directories must be writable by their users. -> while you are able to log in as any of the users ldapuser1 to ldapuser20 the only home directory that is accessible from your system is ldapuserx.

#yum install autofs* -y

#vim /etc/auto.master.d/user.autofs

/home/guests /etc/auto.misc

wq

```
#vim /etc/auto.misc
ldapuser1-ldapuser20     -rw,sync,soft,intr          172.25.254.254:/home/guests/ldapuserx

  wq!
#systemctl restart autofs.service
#su - ldapuserx
#touch file1
#exit
```