**RHCSA EXAM Questions & Answers  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***  
**RHCSA-VM configuration:  
  
\*you have been provided a virtual box named as serverX.example.com (hint:where X is your domain number)  
\* password for both virtual machine should be "Postroll"  
\*serverX.example.com provided with ip=172.25.X.11/255.255.255.0  
\*serverX.example.com are provided with gateway 172.25.254.254 & example.com dns domain with the IP: 172.25.254.254  
  
\*NOTE: I have Foundation Machine# 9, so I am using 172.25.9.11**

nmcli connection add con-name eth0 ifname eth0 type ethernet ip4 172.25.9.11/24 gw4 172.25.254.254  
nmcli connection modify eth0 ipv4.dns 172.25.254.254  
nmcli connection modify eth0 ipv4.method manual  
nmcli connection modify eth0 connection.autoconnect true  
nmcli connection down eth0  
nmcli connection up eth0

----------------------------  
**\* Set the Hostname**

hostnamectl set-hostname server9.example.com

Before starting exam.  
  
**--> ping server-vm ip , desktop-vm ip and classroom.example.com  
--> from server-vm ping base machine and server.  
--> check hostname and IP address of server-vm and desktop-vm**

ping 172.25.9.11  
ping 172.25.9.10  
ping 172.25.254.254  
ping 172.25.254.9 ----> Your base Machine  
ping example.com

**\* if the vm has set with multi-user.target then set it to graphical.target, but don't forget to revert back to multi-user.target**

systemctl get-default --> to check the running target  
systemctl set-default graphical.target

**---> mask the iptable servervice before starting exam.**

systemctl mask iptables.service  
systemctl mask ip6tables.service

**1) configure Selinux**  
  
The machine should be running enforcing mode

vim /etc/selinux/config

Change this

SELINUX=enforcing

Don't forget to Reboot it, so that I'll take affect  
  
**2) create a new 100MB Physical partition mounted under /gluster  
(Note because partition sizes are seldom exactly what is specified when they are created, any thing within the range of 70MB to 120MB is acceptable)**

fdisk /dev/vdb ----- > Create the Partition of 100M  
partx /dev/vdb  
mkfs.ext4 /dev/vdb2 ------> Make a filesystem on it  
mkdir -p /gluster -----> Create Directory to mount on it  
blkid ------> Get the UUID of it  
vim /etc/fstab --------> Create the mount point inside the fstab  
  
UUID=c3ac5a96-80a9-44c3-b51e-9531e9ed9f08 /gluster ext4 defaults 0 0  
  
mount -a ------> Mount it  
df -hT ----> verify it is mounted

**3) create a new 150MB swap partition f/s.  
(Note because partition sizes are seldom exactly what is specified when they are created,  
any thing within the range of 130MB to 170MB is acceptable)**

fdisk /dev/vdb ----- > Create the Partition of 150M and set it's type 82 (which set its the swap type partition)  
partx /dev/vdb --- If you didn't get the partition, just reboot the system, don't get panic  
mkswap /dev/vdb3 ---> Make the swap on newly created Partition  
swapon /dev/vdb3  
swapon -a  
  
vim /etc/fstab --------> Create the mount point inside the fstab  
  
UUID=4f3e868d-c885-4e1f-b069-d56ba443a9b6 swap swap defaults 0 0  
  
Verify:  
  
free -m  
swapon -s

**4) create a repositary for** [**http://content.example.com/rhel7.0/x86\_64/dvd**](http://content.example.com/rhel7.0/x86_64/dvd)

vim /etc/yum.repos.d/rhcsa.repo  
  
[localrepo]  
name = Local Repo for RHCSA exam  
baseurl = [url="http://content.example.com/rhel7.0/x86\_64/dvd"]http://content.example.com/rhel7.0/x86\_64/dvd[/url]  
gpgcheck = 0  
enabled = 1

Test:

yum clean all  
yum list all  
yum repolist

**5) create the following user, groups, and group memberships:  
  
--> A group named sysgrp  
--> A user andrew who belongs to sysgrp as a secondary group  
--> A user susan also belongs to sysgrp as a secondary group  
--> A user sarah who does not have access to an interactive shell on system and who not a member of sysgrp  
--> susan,sarah, andrew password = "Postroll"**

groupadd sysgrp  
useradd andrew  
useradd susan  
useradd -s /sbin/nologin sarah  
usermod -aG sysgrp andrew  
usermod -aG sysgrp susan

Verification:

# id andrew  
uid=1002(andrew) gid=1003(andrew) groups=1003(andrew),1002(sysgrp)  
# id susan  
uid=1003(susan) gid=1004(susan) groups=1004(susan),1002(sysgrp)  
# su - sarah  
This account is currently not available.

**6) create a collaborative directory /redhat/sysgrp with the following characteristics:  
--> Group owneship of /redhat/sysgrpis sysgrp  
--> The directory should be readbale,writable, and accessable to members of sysgrp,  
but not to any other user.  
(It is understood that root has access to all files and directories on the system.  
--> Files created in /redhat/sysgrp automatically have group ownership set to the sysgrp group**

mkdir -p /redhat/sysgrp  
chgrp sysgrp /redhat/sysgrp  
chmod 2770 /redhat/sysgrp

Verification:

# ls -ld /redhat/sysgrp  
drwxrws---. 2 root sysgrp 6 Jun 15 23:21 /redhat/sysgrp

**7) Install the appropriate kernel update from** [**http://content.example.com/rhel7.0/x86\_64/errata**](http://content.example.com/rhel7.0/x86_64/errata) **The following criteria must also be met:  
   -->The updated kernel is the default kerneal when the system rebooted.  
   -->The original kernel remains available and bootable on the system**

vim /etc/yum.repos.d/rhcsa.repo  
  
[kernelrepo]  
name = Local Repo for Kernel  
baseurl = [url="http://content.example.com/rhel7.0/x86\_64/errata"]http://content.example.com/rhel7.0/x86\_64/errata[/url]  
gpgcheck = 0  
enabled = 1

yum repolist

**Run this command before installing the kernel**

uname -rms  
Linux 3.10.0-123.el7.x86\_64 x86\_64

**Install the kernel**

yum install kernel

**After Kernel installation, reboot the system and run this command again**

# uname -rms  
Linux 3.10.0-123.1.2.el7.x86\_64 x86\_64

**8) Enable IP forwarding on your machine**

vim /etc/sysctl.conf  
  
net.ipv4.ip\_forward = 1

**Enable it using:**

sysctl -p

**9) The user andrew must configure a cron job that runs daily at 14:23 local time and executes - /bin/echo hiya**

yum install cronie  
  
systemctl enable crond  
systemctl start crond  
crontab -eu andrew  
  
23 14 \* \* \* /bin/echo hiya

Verification:

crontab -el andrew

**10) Bind with LDAP used provided by classroom.example.com for userr authentication.  
Note the following:-  
--> The LDAP search base DN is dc=example,dc=com  
--> The LDAP certificate file is**[**http://classroom.example.com/pub/EXAMPLE-CA-CERT**](http://classroom.example.com/pub/EXAMPLE-CA-CERT) **-->ldapuserX should be able to log into your system, whereX is your ServerX ((hint:where X is your domain number),  
but will not have a home directory, until you have completed the autofs requirement,below all LDAP users have password of "password"**

yum install authconfig-gtk sssd krb5-workstation  
  
#autoconfig-gtk ---------------------------> Fill the information  
  
systemctl start sssd  
systemctl enable sssd

Verification:

# getent passwd ldapuser9  
ldapuser9:\*:1709:1709:LDAP Test User 9:/home/guests/ldapuser9:/bin/bash  
  
#ssh ldapuser9@localhost

**11) configure autofs to automount the home directories of LDAP users,  
Note the following:  
-->classroom.example.com (172.25.254.254), NFS-exports /home/guests to your system, whereX is your server Number.  
-->LDAP userX's home directory is classroom.example.com:/home/guests/ldapuserX  
-->LdapuserX's home directory should be automounted locally beneath /home as /home/guests/ldapuserX  
-->home directories must be writable by their users  
-->while you are able to login as any of the users ldapuser1 through ldapuser20 the only home directory that is accessible from  
   your system is ldapuserX.  
Example:- classroom.example.com would configure the automaster such that ldapuser100's home directory /home/guests/ldapuserX gets mounted automatically upon login. The NFS share would be classroom.example.com:/home/guests/ldapuser100**

yum install autofs  
  
vim /etc/auto.master.d/home.autofs  
/home/guests /etc/auto.home  
  
vim /etc/auto.home  
ldapuser9 -rw,sync classroom.example.com:/home/guests/&  
  
systemctl enable autofs  
systemctl start autofs

**Verification:**

**#ssh ldapuser9@localhost**  
  
**[ldapuser9@server9 ~]$ df -h**  
Filesystem  Size Used Avail Use% Mounted on  
/dev/vda1   10G 3.4G 6.7G 34% /  
devtmpfs   901M    0 901M 0% /dev  
tmpfs 921M    0 921M 0% /dev/shm  
tmpfs    921M 17M 904M 2% /run  
tmpfs 921M    0 921M 0% /sys/fs/cgroup  
/dev/vdb2   93M 1.6M 85M 2% /gluster  
classroom.example.com:/home/guests/ldapuser9 10G 3.4G 6.7G 34% /home/guests/ldapuser9 --------> This line should be present

**12) Configure your system so that it is an NTP client of classroom.example.com**

yum install chrony  
  
vim /etc/chrony.conf  
  
server classroom.example.com iburst  
  
systemctl restart chronyd  
systemctl enable chronyd

Verification:

chronyc sources -V --> to check the reach level

**13) copy the file /etc/fstab to /var/tmp  
configure the permission of /var/tmp/fstab so that  
the file /var/tmp/fstab is owned by the root user, belongs to the group root  
should not be executable by anyone.  
   The user andrew is able to read & write /var/tmp/fstab  
   The user susan can neighter write nor read /var/tmp/fstab  
   All other users (current or future) have the ability to read /var/tmp/fstab.**

cp /etc/fstab /var/tmp/  
chown root:root /var/tmp/fstab  
setfacl -m u:andrew:rw- /var/tmp/fstab  
setfacl -m u:susan:--- /var/tmp/fstab

Verification:

getfacl /var/tmp/fstab  
  
# su - andrew  
[andrew@server9 ~]$ vim /var/tmp/fstab ----> Try to write anything to the file and it should be successful  
[andrew@server9 ~]$ exit  
logout  
  
# su - susan  
[susan@server9 ~]$ cat /var/tmp/fstab  
cat: /var/tmp/fstab: Permission denied -----> It should show this error  
[susan@server9 ~]$ exit  
logout

**14) Resize the logical volume, logical-data and it filesystem to 400MB.  
Make sure that the filesystem contents remain intact.  
(Note: partitions are seldom exactly  the size requested,so any thing within the range of 370MB to 430MB is acceptable)**

df -Th -------> get the mount point of it

umount /datasource  
e2fsck f /dev/datacontainer/datacopy  
resize2fs /dev/datacontainer/datacopy 400M  
lvreduce L 400M /dev/datacontainer/datacopy  
mount a

**15) Add the user talusan with userid 2985**

useradd -u 2985 talusan

Verification:

# id talusan  
uid=2985(talusan) gid=2985(talusan) groups=2985(talusan)

**find the file which owned by user julice and copy the file into /root/findresults directory.**

mkdir -p /root/findresults  
  
find / -user julice -exec cp -rfp {} /root/findresults/ \;

**16) create a new physical volume, create a new volume group in the name of datacontainer, vg extent is 16.00MB  
create a new logical volume in the name of datacopy with the size of 50 extents and file system must vfat then  
mount it under /datasource**

fdisk /dev/vdb ----- > Create the Partition of 802M[ (16\*50) + 2 ] and set it's type 8e (which is LVM type)  
partx /dev/vdb --- If you didn't get the partition, just reboot the system, don't get panic  
pvcreate /dev/vdb5  
vgcreate -s 16M datacontainer /dev/vdb5  
vgdisplay -----> Check the vg extent size, its should be this (PE Size 16.00 MiB)  
lvcreate -l 50 -n datacopy datacontainer  
lvdisplay ------------> Check the size of extents and it should be(Current LE 50)  
mkfs.vfat /dev/datacontainer/datacopy ------> Make a filesystem on it  
  
mkdir -p /gluster -----> Create Directory to mount on it  
blkid /dev/datacontainer/datacopy -----> get the UUID of /dev/datacontainer/datacopy  
vim /etc/fstab --------> Create the mount point inside the fstab  
  
UUID=C553-2BF5 /datasource vfat defaults 0 0  
  
mount -a

Verification:

df -hT ----> verify it is mounted

**17) create an archive file /root/local.tgz for /usr/local. it should be compressed by gzip.**

tar -cvzf /root/local.tgz /usr/local

**18) search the string sarah in the /etc/passwd file and save the output in /root/lines**

grep sarah /etc/passwd > /root/lines  
  
# cat lines  
sarah:x:1004:1005::/home/sarah:/sbin/nologin