**EXAM QUESTIONS**

1. **Breaking root password**

**Break the root password to have access to the machine. Answer all the questions in your visual machine. The root password should be redhat**

**ANSWER**

**At the grub menu: tap “e” for edit mode**

**Look for the line that has linux16 and go to the end of the line;**

**Tap the space bar and enter: rd.break**

**“ctrl + x” to exit**

**# mount -o remount, rw /sysroot/**

**# chroot /sysroot/**

**# passwd root**

**Enter password**

**Reenter password**

**# touch /.autorelabel**

**# exit(2x)**

**2. Configure your hostname, IP address, Gateway and DNS as follows**

**Host Name: station.domain9.example.com**

**ANSWER**

**# nmtui**

**Edit connection**

**enpOs3**

**manual**

**enter provided IP/24, Gateway, and DNS. (make sure of the following below)**

**X = to require IPv4 addressing for this connection, X = to Automatically connect and X = Available to all users. Scroll down and quit**

**# nmtui**

**Click: Set system hostname**

**Change hostname (as provided in the question), ok and ok**

**# nmtui**

**Activate connection**

**Select enpOs3, tap activate. If already deactivated, do not change. Scroll down and quit or OK**

**# hostnamectl**

**# ping gateway**

**startx**

**3. Configure SELINUX to make it in enforcing mode**

**ANSWER**

**# getenforce**

**# vim /etc/selinux/config**

**SELINUX=permissive**

**:wq!**

**# getenforce**

**4. Configure a default software repository for your system using** File/URL <http://dl.fedoraproject.org/pub/epel/7/x86_64/> (Note: This is my practice link at home)

**ANSWER**

**# yum repolist**

**# cd /etc/yum.repos.d**

**# ls -l**

**# cd**

**# yum-config-manager - -add-repo=http://dl.fedoraproject.org/pub/epel/7/x86\_64/**

**# cd /etc/yum.repos.d**

**# ls -l**

**# vim <filename.repo>**

**gpgcheck=0**

**wq!**

**# yum clean all**

**# yum repolist (should be = or > 4300 in the exam)**

**# cd**

**5. Create User Accounts:**

**Create the users, group and group membership:**

**Create the sysmgrs group**

**A user natasha, using sysmgrs as a sub group**

**A user harry, also using sysmgrs as a sub group**

**A user sarah cannot access the SHELL which is interactive in the system, and is not a member of adminuser, natasha, harry**

**Password for harry, sarah and natasha is redhat**

**ANSWER**

**# groupadd sysmgrs**

**# useradd natasha**

**# usermod -aG sysmgrs Natasha (Thanks to Francisca)**

**# useradd harry**

**# usermod -aG sysmgrs harry**

**# useradd sarah**

**# usermod -s /sbin/nologin sarah**

**# passwd natasha (enter password 2x)**

**# passwd harry (enter password 2x)**

**# passwd sarah (enter password 2x)**

**# grep sysmgrs /etc/group/**

**# tail /etc/passwd**

**6. Configure a User Account**

**Create a user Manalo, uid 3533**

**Password is redhat**

**ANSWER**

**# useradd manalo**

**# usermod -u 3533 manalo**

**# passwd manalo (enter password 2x)**

**# grep manalo /etc/passwd**

**7. Configure NTP (Must be done before cron question)**

**Configure NTP Service, synchronize the server time, NTP server: station.domain9.example.com**

**ANSWER**

**# timedatectl list-timezones | grep America (Steps 1-4, thanks to Francisca)**

**# timedatectl set-timezone America/Chicago**

**# timedatectl set-ntp true**

**# timedatectl restart system-timedated**

**# rpm –qa | grep chrony**

**# yum install chrony -y**

**# vim /etc/chrony.conf**

**station.domain.example.com iburst**

**:wq!**

**# systemctl restart chronyd**

**# systemctl enable chronyd**

**# timedatectl (to verify synchronization. Check time in server to time on desktop. Should match)**

**8. Configure a Cron Task**

**User natasha must configure a cronjob, 14:23 run and execute /bin/echo hiya every day**

**ANSWER**

**# crontab –l –u natasha**

**# crontab -e -u natasha**

**23 14 \* \* \* /bin/echo hiya**

**:wq!**

**# systemctl start crond**

**# systemctl enable crond**

**# systemctl status crond**

**# crontab -l -u natasha**

**9. Upgrade the Kernel**

**Install a suitable Kernel update from** <file://usr/share/pub1/update>**. Following requirement must be met;**

**Updated Kernel used as a default kernel of system start up**

**The original kernel is still valid and can be guided (chosen) when the system start up.**

**ANSWER**

**# uname -r**

**# yum-config-manager - -add-repo=**[**file://usr/share/pub1/update**](file://usr/share/pub1/update)

**# cd /etc/yum/repos.d**

**# vim file.repo**

**gpgcheck=0**

**wq!**

**# yum clean all**

**# yum list kernel**

**# yum install kernel -y**

**# grub2-set-default 0**

**# REBOOT**

**# uname –r**

**# getenforce**

**17. Configure autofs**

**Configure the autofs automatically mount to the home directory of LDAP, as required:**

**Server.domain40.example.com use NFS to share the home to your system. This filesystem contains a pre-configured home directory of user ldapuserX.**

**Home directory of ldapuserX is:**

**Server.domain40.example.com /home/guests/ldapuser**

**Home directory’s of ldapuserX should automatically mount to the ldapuserX of the local /home/guests. The file system is nfs3.**

**Home directory write permission must be available for user**

**Ldapuser1’s password is dynamic (that of Natasha is redhat)**

**ANSWER**

**# yum install autofs nfs-utils -y**

**# vi /etc/auto.master**

**/home/guests /etc/auto.ldapuserX**

**:wq!**

**# vim /etc/auto.ldapuserX**

**\*space-rw,nfs3 station.domain40.example.com:/home/guests/ldapuser /&**

**:wq!**

**# systemctl restart autofs**

**# systemctl enable autofs**

**# systemctl status autofs**

**# mount (should be mounted to /home/guests/ldapuser)**

**16. Binding to an external Validation server**

**System ldap://server.rhatcertification.com provides a LDAP validation service. Your system should bind to this service as require**

**Base DN of validation service is dc=rhatcertification,dc=com**

**LDAP is used to providing account information and validation information connecting and using the certification of** [**ftp://server.rhatcertification.com/pub/slapd.pem**](ftp://server.rhatcertification.com/pub/slapd.pem) **to encrypt**

**After the correct configuration, ldapuser1 can log onto your system**

**It does not have HOME directory until you finish autofs QUESTION.**

**ANSWER**

**# startx**

**# yum install authconfig nss-pam-ldap authconfig-gtk -y**

**# authconfig-gtk**

1. **From the User account database drop down menu; Choose Ldap**
2. **On the LDAP Search Base DN line enter; dc=rhatcertification,dc=com**
3. **Check the box: Use TLS to encrypt connection**
4. **Click on: Download CA Certificate**
5. **Enter provided url in the question**
6. **Go to advanced and check the home directory and Click on apply**

**# systemctl restart nslcd**

**# systemctl enable nslcd**

**# systemctl status nslcd**

**# getent passwd ldapuser (thanks to Francisca)**

**18. Adjust the size of logical volume named vo to 230 MB (instead of 182)**

**ANSWER**

**# df -hT**

**# lvdisplay**

**# lvextend -L 230M -r /dev/myvol/vo**

**# df -hT**

**19. Add a Swap Partition**

**Adding an extra 756M swap partition to your system, this swap partition should mount automatically when the system starts up. Please do not remove or modify the existing swap partitions on your system.**

**ANSWER**

**# free -m**

**# fdisk –l /dev/vd\***

**# fdisk /dev/vda**

**p**

**n**

**enter (default 1st sector)**

**enter (extents, don’t partition)**

**p**

**n (for swap)**

**enter**

**+756M**

**enter**

**t**

**82**

**p**

**w**

**# partprobe (If it returns an error, do: partprobe /dev/vda)**

**# mkswap /dev/vda4**

**# vim /etc/fstab**

**/dev/vda4 swap swap defaults 0 0**

**:wq!**

**# swapon –a**

**# free -m**

**13. Create a logical volume**

**Create a logical volume as required:**

**Name of the logical volume is qa**

**Logical volume size is 60 PE and belongs to volume group named qagroup, with size of 16 MIB per extent. Use ext3 to format this new logical volume.**

**This logical volume should automatically mount to /mnt/qa**

**ANSWER**

**# fdisk -l /dev/vd\***

**# fdisk /dev/vda**

**p**

**n**

**enter**

**+1000M**

**enter**

**p**

**t**

**enter**

**8e**

**p**

**w**

**# partprobe (If it returns an error, do: partprobe /dev/vda)**

**# pvcreate /dev/vda5**

**# pvdisplay**

**# vgcreate -s 16M qagroup /dev/vda5**

**# vgdisplay**

**# lvcreate -l 60 -n qa qagroup**

**# lvdisplay**

**# mkfs.ext3 /dev/qagroup/qa (if it’s vfat, do: mkfs.vfat /dev/qagroup/qa)**

**# mkdir /mnt/qa**

**# vim /etc/fstab**

**/dev/qagroup/qa /mnt/qa ext3 defaults 0 0 (if vfat, enter vfat for fs)**

**:wq!**

**# df -hT**

**# mount –a**

**# df –hT**

**# cd /mnt/qa**

**# echo “I am now a certified RHCSA” > file1**

**# cat file1**

**# cd**

**REBOOT**

**10. Search a String**

**Find out all the columns ‘ismi’ within the /usrs/share/dict/words, then copy all these columns to /root/lists in original order, there is no blank line, all columns must be the accurate copy of the original columns.**

**ANSWER**

**# grep ismi /urs/share/dict/words >> /root/lists**

**# cd /root,**

**# ll,**

**# cat list**

**11. Create a Backup**

**Create a backup file named /root/backup.tar.gz2 that contains the content of /usr/local. Tar must gzip2 to compress.**

**ANSWER**

**# tar - -gzip - -xattrs -cvf /root/backup.tar.gz2 /usr/local/ (Thanks to Francisca)**

**# cd /root,**

**# ll,**

**12. Configure Permission**

**Copy the file: /etc/fstab to /var/tmp/fstab**

**Configure the /vat/tmp/fstab permission as the following:**

**The owner of /var/tmp/fstab is root, belong to group root**

**File /var/tmp/fstab cannot be executed by any user**

**User natasha can read and write /var/tmp/fstab**

**User harry cannot read and write /var/tmp/fstab**

**All other user (present and future) can read /var/tmp/fstab**

**ANSWER**

**# cp /etc/fstab /etc/fstab.bak**

**# cp /etc/fstab /var/tmp/**

**# cd /var/tmp**

**# ll**

**# cd**

**# pwd**

**# chmod a-x /var/tpm/fstab (Thanks to Francisca)**

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

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

**# chmod o+r /var/tmp/fstab**

**# getfacl /var/tmp/fstab**

**13. Create a Share Directory**

**Create a share directory /home/managers, with the following characteristics:**

**/home/managers belong to group sysmgrs**

**This directory can be read, written and accessed by members of the group sysmgrs**

**Any file created in /home/managers group is automatically set as sysmgrs**

**All other user should not be able to access (execute) the /home/managers directory**

**(the user root can always read and write, no matter the permission)**

**ANSWER**

**# mkdir /home/managers**

**# ls –l /home/**

**# chown :sysmgrs /home/managers**

**# chmod g+rwxs /home/managers**

**# chmod o-x /home/managers**

**# getfacl /home/managers**

**# cd /home/managers**

**# pwd**

**# touch file2**

**# ll**

**# cd**

**14. Search Files**

**Find a file owned by natasha, (it could be any name), and copy them to a directory /root/findfiles**

**ANSWER**

**# mkdir /root/findfiles**

**# find / -user natasha -exec cp -a {} /root/findfiles \;**

**# cd /root**

**# cat findfiles**

**# pwd**

# REBOOT

**YOU ARE NOW RED HAT CERTIFEIED THROUGH THE BLESSINGS OF YOUR ANCESTORS!**