RHCSA (EX200) EXAM PAPER

NOTE: - Two new virtual machines will be given for RHCSA Exam Paper. All perform in your virtual Machine. Your exam code isEX200. (node1 and node2 machine)

After login to the base machine, you are to see an **Activities** on base machine in which information regarding:

1. RedHat icon will show your question paper and give you basic instructions like Node1 machine root password.
2. Below that we have a VM icon, which we will allow us to open both the machines Node1 and Node2, we can start them and click on open console to get a proper view, with half screen question paper and half as VM terminal.

Perform all in your virtual system. DO NOT change the physical machine root password. Do not access your physical machine root user. You can log in as a limited user.

After booting and accessing the console of Node1, you are to login as root and given password and run the command 'startx' to get the GUI interface for further working.

Q1.) Setup Networking for Node1

ip address: 172.25.10.11
subnet mask: 255.255.255.0
Default gateway: 172.25.10.254
nameserver: 72.25.254.254
hostname as primary.netX.example.com

Ans. Network Configurations

nmtui (for set the IP address)

Edit a Connection --> select Wired Connection1 (eth0) --> go to IPV4 CONFIGURATION --> select Manual --> show

Enter on Add Addresses = 172.25.10.11/24
Gateway = 172.25.10.254
DNS = 172.25.254.254

Do, Okay and exit the part
Then turn the connection down and then once up.

For Hostname:

hostnamectl set-hostname primary.netX.example.com [to set hostname]

hostname [to verify hostname]

ping 172.24.0.110 [To Verify]

ip addr [To Verify changes are applied]

Q2.) Yum repository configuration on Node1

Ans.

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

[BaseOS]

baseurl = http://content.example.com/rhel8.0/x86_64/dvd/BaseOS

enabled = true

gpgcheck = false

[AppStream]

baseurl = http://content.example.com/rhel8.0/x86_64/dvd/AppStream

enabled = true

gpgcheck = false

:wq!

yum repolist [To verify]

yum install httpd [To verify]

Q3.) Debug SE-Linux

http service serves non-standard *82* port for your machine, the system is not able to connect to httpd service at port 82, fix the debug issue, to store the *HTML* files under */var/www/html* directory don't have change to it. it should be accessible at *port 82* and should start at boot time.

ANS

semanage port –a –t http_port_t –p tcp 82 (add port on SE-Linux policy)

#systemctl restart httpd

systemctl enable httpd

firewall-cmd -- permanent – add-port=82/tcp (add port to firewall)

firewall-cmd –reload

To Match the secontext in /var/www/html

ls -lZ /var/www/html

chcon -t http_system_t /var/www/html/file1 (Whichever file has different context)

Q4.) Configure a cron job on Node1

a. The user natasha must configure a cron job that runs daily at 13:30 local time and executes /bin/echo hello

OR

b. The user natasha must configure a cron job that runs daily at every 3-minute local time and executes /bin/echo hiya

useradd natasha (to add the user)

crontab -e -u natasha (to add the following line)

30 13 * * * /bin/echo hello

*/3 * * * * /bin/echo hiya

:wq

```
# systemctl restart crond                    (to restart the service)
# systemctl enable crond                     (to enable the service)
# crontab -l  -u natasha                     (to check)
```

Q5.) Create the following users, groups, and group memberships

A group named sysadmin. A user natasha who belongs to sysadmin as a secondary group. A user sarah 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. Natasha, Sarah and Harry should all have the password of atenorth.

Ans. We're going to create users, group and group membership with following steps-

Step-1. groupadd sysadmin -> This command is simply creating a group "sysadmin" in which no any member added recently.

Step-2. useradd (username) -> By this command, we'll create user with given name of user.

Step-3. usermod –aG (group_name) (user_name) -> By this command, we'll add user into a group as secondary group of user because when user created then primary or personal group of user automatically created so another group is treated like secondary group for user. -> In this command, "-a" option is used for append user with secondary group and "-G" option is used to specify group which user will be append and with "-G" option, we specify the group name and at last, we give thename of user which will be append with secondary group.

OR

useradd -G (groupname) (username) to add it in single command

Step-4. useradd –s /sbin/nologin (user_name) -> In this command, we'll create a user with given name which not have access on interactive shell. -> In this command, "-s" option is used to provide any required shell to any user.

Step-5. passwd (user_name) -> This command is used to give password to any user.

Q6). Create a collaborative directory "/common/admin" with the following characteristics

Group ownership of /common/admin 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 /common/admin automatically have group ownership set to the sysadmin group.

Ans. We're going to create collaborative and also give group ownership and permission for group members-

Step-1. mkdir –p (path of directory) -> In this command, we're creating a collaborative directory with "mkdir" command which is used to make directory. -> In this command, "-p" option is used to make parent directory of current directory simultaneously. -> With "mkdir" command and "-p" option, we'll give directory name with parent directory name like "/common/admin" and both directories will createsimultaneously.

Step-2. chgrp (group_name) (path of directory) -> This command is used to change group ownership of any directory.

Step-3. chmod 2770 (path of directory)

-> "chmod" command is used to give permission to root, group or any other user. -> In this command, after "chmod" command first digit which is "2" is used to give special permission which is SGID by which all files in "/common/admin" directory automatically have group ownership and second digit which is "7" is used to give read, write and access to root user and third digit which is "7" is used to give read, write and access to group and last digit which is "0" is used to give no any permission of read, write and access to any other user. -> At last, we give path of directory on which we want to give permission.

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

vi /etc/chrony.conf

Comment the line no. 3 of starting with the pool.

pool 2.rhel.pool.ntp.org iburst (comment this line)

server utility.domain0.example.com iburst (add the line)

:wq

systemctl restart chronyd

systemctl enable chronyd

chronyc sources [To Verify]

Q9). Find the files in your system which is owned by Simone user & copy all the files on /root/found directory

Step-1. mkdir (path of new directory) -> By “mkdir” command, We make a new directory where we cancopy all find files.

Step-2. find / -user (user_name) –exec cp –aprvf {} (path of directory where we want to copy) \; ->

Ex.

find / -user natasha -exec cp -aprvf {} /root/found \;

“find” is a command to find any file or directory. -> After the “find” command, we use “/” which means this command will find the required file in whole system because whole directory or file is made in “/”. -> After “/”, We use “-user” option which is used to specify the name of user and we’re using this option when we want to find that files which is owned by any user. -> After specify the user name, we use “–exec” option by which we can add or join another command with previous command. -> After the “-exec” option, we use “cp” command for copy all files at given path of directory. In “cp” command, we use certain following option- -a = This option is used to append command with previous command. -r = This option is used to copy files recursively. -v = This option is used to print verbose information on screen means process shows on display. -f = This option is used to copy all files forcefully. -> After all options, we give path of that directory where we want to copy all file which is find and owned by specified user.

Go to directory to verify the changes

Q. 10 Configure AutoFS

● All remoteuserX home directory is exported via NFS, which is available on node1.domainX.example.com (172.25.254.254) and your NFS- exports directory is /rhome for remoteuserX,

● remoteuserX's home directory is node1.domainX.example.com:/rhome/remoteuserX

● remoteuserX's home directory should be automount autofs service.

● Home directories must be writable by their users.

● The only home directory that is accessible from your system is remoteuserX

Ans.

Step-1. yum install -y autofs -> By this command, we're going to install autofs package to configure remoteuser.

Step-2. vim /etc/auto.master.d/(file_name).autofs -> By this command, we create a new file in "/etc/auto.master.d/" in which we specify the home directory for remoteuser and also specify the path of a file which is "/etc/auto.misc".

Here the entry will be

/- /etc/auto.misc

Step-3. vim /etc/auto.misc -> By this command, we open the file which is "auto.misc" in which we specify the information in below syntax-

remoteuserX -rw,soft,intr servername:(full path of home directory of remoteuser)

Step-4. systemctl start autofs ; systemctl enable autofs -> In this step, First command is used to start "autofs" service in system. -> Second command is used to enable the "autofs" service by which after the reboot of system, service will automatic start.

Step-5. su – remoteuserX -> This command is used to switch user and by this command, we can login on remoteuserX shell prompt and also can verify that remoteuserX is created or not. This is to verify.

Step-6. pwd -> "pwd" command is used to check present working directory and by this command, we also check that remoteuserX have his home directory or not which is provided by server to remoteuserX.

Q12.) User of Specific UID

Create a user *barry* User id of this user should be *2112* and set password *atenorth*

useradd -u 1220 barry

#passwd barry

id –u barry [To Verify]

Q 13 Sudo privilege

a group name is '*elite*', they have to give administrative permission without password.

visudo

Add the new line
%elite ALL=(ALL) NOPASSWD: ALL
:wq

Q14. Create a archive file using gz compression
(a) Backup the /var/tmp as /root/data.tar

#tar –zcvf /root/data.tar /var/tmp
Variations: (-J for xz, -j for bz2, -z for gz)
#ls /root

Q. 15. Set the Password expire date
The password for all new users in node1.domain18.example.com should expires after 20 days.

#vim /etc/login.defs

PASS_MAX_DAYS 20

Esc:wq

Q16. Copy 'wired' /usr/share/dict/words to the directory /tmp/data

#grep 'wired' /usr/share/dict/words > /tmp/file
cat /tmp/file

Q17. Write a script "mysearch" to list the contents of /usr that are smaller 10M and have SGID permission
The script should be present in /usr/local/bin
After execution, the script should automatically write and save to /root/found

#mkdir /root/found
#vim mysearch

#!/bin/bash

find /usr -size -10M -perm /2000 > /root/found
:wq

chmod a+x mysearch
cp mysearch /usr/local/bin
mysearch

14.) Container Related Questions

1) As Andrew user, build an image from following link using and name it watcher
http://server1.net3.example.com/materials/3/Containerfile

Ans.

ssh andrew@localhost

Containerfile

wget http://server1.net3.example.com/materials/3/Containerfile

podman build -t watcher .

Podman image ls [To Verify]

2) create a container using the image you created

- create a container using Andrew user
- container name should be watcher
- mount /opt/files directory to /opt/incoming in container and /opt/processes to /opt/outgoing in container
- container should run as a system service, so configure as a service name container-watcher.service
- container should run at boot time

this container will convert ascii text file into pdf format, so when you create simple file in /opt/ files then container will automatically convert that file into pdf and save /opt/processes

Ans.

As root user:

mkdir -p /opt/files
mkdir -p /opt/processes
chown Andrew:Andrew /opt/files
chown Andrew:Andrew /opt/processes

Now switch to Andrew user
ssh Andrew@localhost

Podman run -d –name watcher -v /opt/files:/opt/incoming:Z -v /opt/processes:/opt/outgoing:Z watcher

Podman ps [To Verify]

Now in Andrew home directory

mkdir -p .config/systemd/user

cd .config/systemd/user

Podman generate systemd –name watcher –new –files

systemctl –user daemon-reload

systemctl –user enable container-watcher.service

systemctl –user start container-watcher.service

loginctl enable-linger

NODE 2

Q1.) First step is to crack password of Secondary Machine.

Ans. crack password of virtual machine for root

**** You have to reset your root password *****

1:- Just restart your virtual machine (Click on Ctrl + Alt + Delete button)2:- Press space bar key (to stop the GRUB line)

3:- select 2nd line press "e" (to edit the grub)

4:- go to end of linux line (press END key)

5:- just give space and type rd.break (type the command)6:- Press ctrl+x (to start)

Give the root password for maintenance (Press Enter)

mount -o remount,rw /sysroot

chroot /sysroot

passwd root

touch /.autorelabel

exit

exit

Q2.) Yum repository configuration on Node 2 as well

Ans.
vim /etc/yum.repos.d/new.repo

[BaseOS]

baseurl = http://content.example.com/rhel8.0/x86_64/dvd/BaseOS

enabled = true

gpgcheck = false

[AppStream]

baseurl = http://content.example.com/rhel8.0/x86_64/dvd/AppStream

enabled = true

gpgcheck = false

:wq!

yum repolist

Q3). Set a recommended tuning profile for your system. (Profile already available)

Ans- Use yum to confirm that the tuned package is installed

yum install tuned

Use the systemctl is-enabled tuned command to display the tuned service enablement state

systemctl enable --now tuned

To check which profile to be used

tuned-adm recommend

#tuned-adm profile <name of recommended profile>

tuned-adm active [To verify]

Q4). Create a SWAP partition of 250 megabyte and make available at next reboot. Partition already available.

```
# fdisk -l

# fdisk /dev/vda                                  (create partition)

n
1
<blank>
+250M
t
swap
w

# mkswap  /dev/vda4                    (make swap partition)

# swapon/dev/vda4                      (to enable swap)

#vim /etc/fsatb

/dev/vda4        swap            swap        defaults    0    0

:wq

# mount –a                             (to check syntax)

# swapon –s                            [to check]
```

Q5). Create the volume group with name myvol with 8 MiB P.E. and create the lvm name mydatabase with the 50 P.E. and format this lvm with ext3 and create a directory /database and mount this lvm permanently on /database.

```
# fdisk /dev/vda

n
1
<blank>
+1G
t
lvm
w


 # pvcreate /dev/vda5

 # vgcreate -s 8M datastore  /dev/vda5
```

vgcreate -s 8M myvol /dev/vda5

lvcreate -l 50 -n database datastore

lvcreate -l 50 -n mydatabase myvol

mkfs.ext3 /dev/datastore/database

mkfs.ext3 /dev/myvol/mydatabase

mkdir /mnt/database

vim /etc/fstab

Insert the line last line of the file

/dev/datastore/database /mnt/database ext3 defaults 0 0

:wq

mount -a [To Verify]

lsblk -f [To Verify]

Q6). Resize the Lvm partition "home" to 150MiB.

Ans. We're going to resize the LVM partition with some following steps-

Step-1. lvdisplay -> "lvdisplay" command is used to show the created LVM partition by which we can see the details of created LVM partitions.

Step-2. lvextend -r –L (required_size in Kb or Mb or Gb) (path_of_LVM_partition) -> "lvextend" command is used to extend lvm partition with required size of partition. -> With this command, we use "-L" option which is used to extend or set size of partition in form of kilobyte, megabyte or gigabyte and many more. If we use "+" sign with value then value is added in actual size of partition but if we not use "+" sign with value then value is set as actual size of LVM partition. -r will ensure that this is formatted as per the same filesystem of complete lvm saving us the task to do so

lvresize -r -L 150M /dev/myvol/mydatabase