RHCSA(EX200) EXAM-PAPER

- Three machines are there on your exam environment

1. Base Machine – base.net.example.com
    a. Primary – primary.netX.example.com
    b. Secondary – secondary.netX.example.com

On Primary Machine:

Q1.) setup an ip address for Primary virtual machine.

ip addr 172.25.X.11 subnet mask 255.255.255.0 Default gateway 172.25.X.254 nameserver 172.25.254.254 and hostname as primary.netX.example.com.

Ans. Network Configurations

1. Nmcli con show (It show active connection)
2. Nmcli con modify "System eth0" ipv4.address "172.25.X.11/24 172.25.X.254" ipv4.dns 172.25.254.254 ipv4.method static
3. Nmcli con down "System eth0"
4. Nmcli con up "System eth0"
   Set hostname: hostnamectl set-hostname serverX.example.com.

Cross Check: run command nslookup server.example.com if it show your IP then network work proper.

- Key in **startx** to go in the GUI mode

Q2.) Yum repository configuration on both machines

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.) Configure a cron job on Primary machine

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

OR

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

Ans. We're going to schedule a job in our system. By this, we can schedule a job which automatically perform a task on configured time by some following steps-

Step-1. **crontab –eu (user_name)** -> "crontab" is a command which is used to schedule the job on time. -> In this, we use following two options- -e = This option is used to assign the job with time -u = This option is used to give user name by which we can specify the job for specific user.

Step-2. After the execution of above command, one file is open on screen where we have to fill proper entry with given syntax- *** * * * *** (Task which we want to assign to user) -> First (*) is for every minute :- Means task will be perform on each and every minute if we substitute * on this place instead of any numeric value (range 0-59). -> second (*) is for every hour :- Means task will be perform on each and every hour if we substitute * on this place instead of any numeric value (range 0-23). -> third (*) is for every day of month:- Means task will be perform on each and every day if we substitute * on this place instead of any numeric value (range 1-31). -> fourth (*) is for every month :- Means task will be perform on each and every month if we substitute * on this place instead of any numeric value (range 1-12).

-> fourth (*) is for every week's day :- Means task will be perform on each and every week's day if we substitute * on this place instead of any numeric value (range 1-12). -> After full fill entire entry according to syntax then save the file and exit.

Step-3. **crontab –u (user_name) -l** -> This command is used to show job scheduling for specified user. -> In this command, "-u" option is used to specify user and after specify the user name, "-l" option is used to show job scheduling for specified user.

Q5.) SELinux must be running in the Permissive mode. (given in instructions)

Ans. We're going to set our system on enforcing mode because this is special type of security which is "Security Enhance Linux" by which we can implement a flexible mandatory access control architecture in our system. We can do this by some following steps-

Step-1. **getenforce** -> This command is used to get current mode of SELinux.

Step-2. **setenforce 0** -> This command is used to modify the mode of SELinux on run time. -> After the "setenforce" command, "0" is used for permissive mode for SELinux. We can also place "1" on place of "1" for enforcing mode for SELinux.

Step-3. **vim /etc/selinux/config** -> We'll open config file of SELinux with above command and do entry for enforcing mode in file. We write permissive on place of enforcing entry in front of "SELINUX=" and save the file. -> We do this step because when system will reboot then system read this file and automatically set permissive mode for SELinux.

Q6.) 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 thuctive.

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 in

which user will be append and with “-G” option, we specify the group name and at last, we give the name of user which will be append with secondary group.

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.

Q7). 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 directory will created simultaneously.

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). 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 belong 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 sarah can neither write nor read /var/tmp/fstab. [Note: all other users (current or future) have the ability to read/var/tmp/fstab.]

Ans. Now We're going to copy the file /etc/fstab to /var/tmp and also give some permission according to requirement. We can done this thing with some following steps-

Step-1. **cp (path of file which we want to copy) (path of directory where we want to copy)** -> "cp" command is used to copy any file or directory. -> After "cp" command, we give path of that file which we want to copy and after this we give path of that directory where we want to copy file.

Step-2. **ll (path of copied file)** -> "ll" command is used for long listing of any file or directory means this command show the full detail of any file or directory. With help of "ll" command, we can see the owner of file, group owner of file and also we can see the current permission on file for users. -> By default, owner and group owner of "fstab" file is root.

Step-3. **chmod 771 (path of copied file)** -> "chmod" command is used to change file mode or change the permission of file. After the command, First digit which is "7" is for root user which means root user have all permission on file and second digit which is "7" is for group owner which means group owner also have all permission on file and last digit which is "1" is for other users which means other user have read permission on specified file.

Step-4. **setfacl –m u:(user_name):rwx (path of copied file)** -> "setfacl" command is used for set file access control lists means some special permission for specified user on specified file. -> In this command, "-m" option is used for modifying configuration in ACL file or directory. -> After the option, There're three field in command which all separated by ":". In these three field, first is "u" which specify that we want to give special permission on file for particular user. -> Second field is "user_name" in which we give name of user. -> Third field is "rwx" in which we specify the permissions for particular user on particular file. -> By this whole command, we can give any special type of permission to any user on any particular file.

Q9). Configure NTP in your system so that it is an NTP client of classroom.example.com.

Ans. We're going to synchronize the system time with server time or configure the Network Time Protocol because if system time is not synchronized with server time then we can face some problem in accessing of server from system. We can configure the NTP with some following steps-

Step-1. **vim /etc/chrony.conf** -> First, we open the file “chrony.conf” with help of vim editor. In this .conf file, we write some entry related to server with given syntax- **server (hostname) iburst** -> After fill the proper entry in “chrony.conf” file then save it.

Step-2. **systemctl restart chronyd.service ; systemctl enable chronyd.service** -> In this step, we’ll restart the service of “chronyd.service” and enable this service by which all configuration will remain same after reboot of system.

Step-3. **chronyc sources –v** -> By this command, we can cross check the connection with server and also can check that system time is synchronized with server time or not.

Q10). Find the files in your system which is owned by Simone user & copy all the files on /root/found directory

Ans. We’re going to find the files in system and copy all the find files in specified directory. We can do this task with some following step-

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

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

Step-3. **ll (path of that directory where all file copied)** -> By this “ll” command, we can cross check that “find” and “cp” command will done work properly or not.

Q11). Find the string strato from /usr/share/dict/words/file and save the result in /searchfile.

Ans. We're going to search a particular string from a particular file and store output into specified file with some following steps-

Step-1. **grep 'strato' (path of that file in which we want to search string) > (path of that file in which we want save output)** -> "grep" is a command to search specified string in command (eg. 'strato') this string is always written in single quotes(' ') after the command. -> After the "grep" command, We provide the path of that file in which we want to search string and after this, we use ">"(redirection) to save output of "grep" command into specified file.

Step-2. **vim (path of that file where we save the output of command)** -> With use of vim editor, We can open file in which output will save and cross check the result.

Q12.) Using automounter service mount RemoteuserX onto the provided folder /ourhome/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**".

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 -(permission),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.

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.

On Secondary Machine:

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

Ans. crack password of virtual machine for root

Step-1. when our virtual machine selecting the kernel in starting then there is a option for editing by pressing “**e**” button on keyboard by which we can done editing in between booting process and also able to crack password of root.

Step-2. when we’re in editing mode by pressing “e” button then there’s a coding on screen. when you’ll go down in coding then there’s a line which started by “linux16/”. In this end of line, we write “**rd.break**” and press “**Ctrl + x**” by which booting will start again and give a command line interface where we can run further commands which is required to crack password of root.

Step-3. On command line interface, we write command- **mount -o remount,rw /sysroot** -> By this command, we’re going to remount with read and write permission on “/sysroot”. -> In this command,”-o” option is used for give option for remount.

Step-4. **chroot /sysroot** -> By this command, we get an interactive shell with special root directory because we want an interactive shell on which we can easily run command to change password of root.

Step-5. **passwd root** -> This is command for changing password of any user so we’re going to change password of root.

Step-6. **touch /.autorelabel** ->

Step-7. **Exit** -> Now by write “exit” on command line by which we can exit from interactive shell.

Step-8. **Exit** -> Now again we write “exit” on command line interface by which we can exit from command line interface and booting process will again started with new root password.

Q2.) Yum repository configuration on both machines

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 is-enabled tuned enabled

List all available tuning profiles and their descriptions

 # tuned-adm list

Mention the profile to be loaded

 # tuned-adm recomended

 # tuned-adm active

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

Ans. We're going to create a swap partition by which we can give supportive memory to RAM. We can do this task with some following steps-

Step-1. Initially we create a new partition according to required size of partition but when we're going to save partition by press 'w' before that we have to change the partition type by press 't'. When we press 't' then we have to give hex code(82) of "Linux swap partition type" and press enter. If we have any confusion then we can check the hex code of "Linux swap partition type" by press "l".

Step-2. **mkswap (path of swap type partition)** -> "mkswap" is command to format new swap partition by which we can activate the swap partition on run time.

Step-3. **swapon (path of swap type partition)** -> "swapon" command is used to active swap partition on run time.

Step-4. **free –m** -> "free" command is used to check or display free and used amount of memory in system. -> "-m" option is used to display free and used amount of memory in system in Megabyte(mb).

Q5). Create the volume group with name myvol with 8 MiB P.E. and create the lvm name mydatabase with the 100 P.E. and format this lvm with vfat and create a directory /database and mount this lvm permanently on /database.

Ans. We're going to perform above question with given requirements-

Step-1. In first step, we have to create a normal partition with "Linux LVM" by providing "8e" hex code.

Step-2. **pvcreate (path of created partition of LVM type)** -> With help of "pvcreate" command, we're creating a physical volume of LVM type partition by which we can create volume group of physical volume.

Step-3. **vgcreate -s (size of P.E.) (V.G. name) (path of P.V. partition)** -> With help of "vgcreate" command, we're creating volume group by physical volume partition and we can add one or more physical volume in a single volume group to increase size of volume group by other command. -> After the "vgcreate" command, we use "-s" option by which we can set the physical extent size on physical volumes of specified volume group. By default, P.E. size is 4Mb. -> We can check the all created volume group by "vgdisplay" command.

Step-4**. lvcreate –L (size of L.V.) –n (name of L.V.) (path of V.G.)** -> With help of "lvcreate" command, we're creating logical volume from volume group. -> After the command, we use some following

options- -L = This option is used to provide size of new logical volume. -n = This option is used to give name of new logical volume. -> We can check the all created logical volume by “lvdisplay” command.

Step-5. **mkfs.(file_system) (path of newly created logical volume partition)** -> “mkfs” command is used to make file system of any partition and by separating “.”, we provide file system which we want to provide to new logical volume partition. After the command, we give path of that L.V. partition which we want to format.

Step-6**. vim /etc/fstab** -> In this step, we have to mount L.V. partition of given mount point by fill the entry in “/etc/fstab” file for permanent mounting.

Step-7. **mount -a** -> We have to reboot our system or run “mount -a” command by which partition will be mount on specified mount point. In this command, “-a” is used of mount all that partition on specified mount point which we specified in “/etc/fstab” file for permanent mounting.

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 –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.

Step-3. **resize2fs (path_of_LVM_partition)** -> “resize2fs” command is used to resize the ext2/ext3/ext4 file system after extend the size of LVM partition. It’s used to enlarge or shrink a mounted or unmounted file system located in system.

Step-4. **lvremove (path_of_LVM_partition)** -> “lvremove” is used to remove any created LVM partition and after this command, we give path of LVM partition which we want to remove.

Q7). You have been provided with a disk drive attached to your system, make use of it to create a VDO device with a logical size of 50GB.

Ans.

Step-1. yum install vdo kmod-kvdo -> Install the vdo and kmod-kvdo packages to enable VDO in the system.

Step-2. vdo create --name=vdough --device=/dev/vdd --vdoLogicalSize=50G -> This creates a VDO volume, named vdo1 with the given drive and of a logical volume.

Step-3. vdo start --name=vdough ; . vdo stop --name=vdough ; vdo status --name=vdough, This displays the list of VDO volumes that are currently started. You can start and stop a VDO volume using the vdo start and vdo stop commands, respectively.

Q8). Create a backup.tar.(bz2 or gz) of /etc directory in /home location.

Ans. We're going to create a backup of given directory on specified location with some following steps-

Step-1. **tar –cvfj (file_name.tar.bz2 { or -z for gzip file })** (path of that directory where we want to save backup file) -> "tar" command is used to create backtup of any file or directory. -> With "tar" command, we use some following options: -c = This option is used to create a new archive. -v = This option is used for verbosely list files processed (display processing on screen) -f = This option is used for creating backup in a single file. -j = This option is used for .bzip2 compression technique or -z = This option is used for .bzip2 compression technique. -> After providing the option, We provide the file name of .tar file and after this we provide path of that directory where we want to save .tar file.

Step-2. **ls (path of that directory where we saved the backup file)** -> "ls" command is used to show file of any directory