Practice Test 6 RHCSA (EX200)

Question 1

1. Assume that you forget the root password. Reset the root password for ServerC. Change it to “watchword” to gain access to the system.
   - `e`
   - `rd.break`
   - `mount -o remount rw /sysroot`
   - `chroot /sysroot`
   - `passwd root`
   - `touch /.autorelabel`
   - `exit`
   - `reboot`

Question 2

2. On ServerC, configure your system to use the YUM repositories available from:
   - http://ServerB/dvd/BaseOS
   - http://ServerB/dvd/AppStream
   as the default repository.

```
On ServerB:
- `cd /var/www/html/`
- `mkdir dvd`
- `mount /dev/sr0 dvd`
- `ifconfig`

On ServerC:
- `cd /etc/yum.repos.d/`
- `cat redhat.repo`
- `mv redhat.repo /home`
- `vi serverB.repo`
```

File editor:

```
[BaseOS]
name = BaseOS Packages Red Hat Enterprise Linux 9
metadata_expire = -1
gpgcheck = 0
enabled = 1
baseurl = http://ServerB/dvd/BaseOS

[AppStream]
name = AppStream Packages Red Hat Enterprise Linux 9
metadata_expire = -1
gpgcheck = 0
```

```
enabled = 1
baseurl = http://ServerB/dvd/AppStream
```

- - `subscription-manager clean`
  - `dnf clean all`
  - `dnf repolist`
  - `dnf install update`

Question 3

3. Change ServerC hostname to ServerB and make it persistent.
   - `vi /etc/hostname`
     - Change line to: `ServerB`
   - `reboot`

Question 4

4. On ServerB, modify your active network interface configuration to follow the following specifications statically:
   - IPV4 – 192.168.1.7/24
   - GW – 192.168.1.1
   - DNS – 8.8.8.8
   - `nmcli connection modify enp0s3 ipv4.addresses 192.168.1.7/24`
   - `nmcli connection modify enp0s3 ipv4.gateway 192.168.1.1`
   - `nmcli connection modify enp0s3 ipv4.dns 8.8.8.8`
   - `nmcli connection enp0s3 && nmcli connection up enp0s3`

Question 5

5. On ServerB, add the following secondary IPV4 address statically to your current running interface. Do this in a way that doesn't compromise your existing settings:
   - IPV4 – 10.0.0.7/24
   - `nmcli connection modify enp0s3 +ipv4.addresses 10.0.0.7/24`
   - `nmcli connection enp0s3 && nmcli connection up enp0s3`

Question 6

6. On ServerB, add the following IPV6 address statically to your current running interface. Do this in a way that doesn't compromise your existing settings:
   - IPV6 – fd01::107/64
   - `nmcli connection modify enp0s3 +ipv6.addresses 10.0.0.7/24`
   - `nmcli connection enp0s3 && nmcli connection up enp0s3`

Question 7

7. Enable IPV4 packet forwarding on ServerB. This should persist after a reboot.
    - `sysctl net.ipv4.ip_forward`
    - `vi /etc/sysctl.conf`
        - Add the line: `net.ipv4.ip_forward = 1`
    - `sysctl -p`

Question 8

8. Enable IPV6 packet forwarding on ServerB. This should persist after a reboot.
    - `sysctl net.ipv6.conf.all.forwarding`
    - `vi /etc/sysctl.conf`
        - Add the line: `net.ipv6.conf.all.forwarding = 1`
    - `sysctl -p`

Question 9

9. On ServerB, set the system time to the "America/Chicago" timezone.
    - `timedatectl`
    - `timedatectl set-timezone "America/Chicago"`

Question 10

10. On ServerB, ensure NTP sync is configured.
    - `systemctl status chronyd`
    - `vi /etc/chrony.conf`
    - `systemctl restart chronyd`
    - `timedatectl set-ntp true`
    - `chronyc`
        - `sources`

Question 11

11. ServerB should boot into the graphical.target by default.
    - `systemctl get-default`
    - `systemctl set-default graphical.target`

Question 12

12. On ServerB, create a user john with UID 1250 and expiry date 2023-12-21.****
    - `useradd -u 1250 -e 2023-12-21 john`
    - `id john`
    - `chage -l john`

Question 13

13. On ServerB, create a new file “/tmp/tmpfile”, so that it is owned by the user leo, and belongs to the group science, then do the following:
    - All users can execute the "/tmp/tmpfile" file.
    - The "/tmp/tmpfile" file should not be writable by anyone.
    - The user james is able to read, write, and execute the "/tmp/tmpfile" file.
    - `touch /tmp/tmpfile`
    - `useradd leo`
    - `groupadd science`
    - `chown leo:science /tmp/tmpfile`
    - `chmod a+x /tmp/tmpfile`
    - `chmod a-w /tmp/tmpfile`
    - `ls -l /tmp/tmpfile`
    - `useradd james`
    - `setfacl -m u:james:rwx /tmp/tmpfile`
    - `getfacl /tmp/tmpfile`

Question 14

14. On ServerB, use /dev/sdb to do the following:
    1. Create a 4GB volume group named “vg6”.
    2. Create a 2G logical volume named “lv6” inside the “vg6” volume group.
    3. The “lv6” logical volume should be formatted with the ext4 filesystem and mounted persistently on the “/lv6” directory.
    4. Extend the ext4 filesystem on “lv6” by 500M.
    - `lsblk`
    - `fdisk /dev/sdb`
        - `p` `n` `p` `1` `Enter` `+4G` `p` `l` `t` `1` `8e` `p` `w`
    - `lsblk`
    - `pvcreate /dev/sdb1`
    - `vgcreate vg6 /dev/sdb1`
    - `vgs`
    - `lvcreate -L 2G -n lv6 vg6`
    - `lvdisplay`
    - `mkfs.ext4 /dev/vg6/lv6`
    - `blkid`
    - `vi /etc/fstab`
        - Add the line: `/dev/mapper/vg6-lv6 /lv6 ext4 defaults 0 0`
    - `mkdir /lv6`
    - `mount -a`
    - `df -h`
    - `lvextend -L +500M /dev/vg6/lv6`
    - `lvs`

Question 15

15. On ServerB, using disk /dev/sdb, do the following:

- Create a 1T thin provisioned volume "thinvol1" under the 2G thin pool "thinpool1" in the 3G volume group "vg1".
- Extend the size of "thinpool1" by 500M.
- Rename the thin pool from "thinpool1" to "thinpool2".
- Rename the thin provisioned volume from "thinvol1" to "thinvol2".
- `lsblk`
- `fdisk /dev/sdb`
  - `p` `n` `p` `2` `Enter` `+3G` `p` `l` `t` `2` `8e` `p` `n`
- `lsblk`
- `pvcreate /dev/sdb2`
- `vgcreate vg1 /dev/sdb2`
- `lvcreate --thinpool thinpool1 -L 2G vg1`
- `lvs`
- `lvcreate -T -V 1T -n mythinvool1 vg1/thinpool1`
- `lvs`
- `lvextend -L +500M /dev/vg1/thinpool1`
- `lvrename /dev/vg1/thinpool1 thinpool2`
- `lvrename /dev/vg1/thinvol1 thinvol2`
- `lvs`

Question 16

16. On ServerB, optimize the system to run in a virtual machine for the desktop use-case tuned profile.
    - `systemctl enable tuned --now`
    - `tuned-adm active`
    - `tuned-adm list`
    - `tuned-adm profile virtual-guest desktop`
    - `tuned-adm active`

Question 17

17. On ServerB, configure Apache to serve a basic website that shows the text "Hello World!"
    - `dnf install httpd -y`
    - `systemctl enable httpd --now`
    - `firewall-cmd --list-all`
    - `firewall-cmd --add-service=http --permanent`
    - `firewall-cmd --reload`
    - `firewall-cmd --list-all`
    - `vi /var/www/html/index.html`
      - Add the line: `Hello World!`
    - `curl http://localhost`

Question 18

18. On ServerB, find regular files owned by the user root in “/usr/” and copy the files into the “/find/rootfiles/” directory.
    - `find /usr -type f -user root -exec cp {} /find/rootfiles/ \;`
    - `ls -ltr /root/rootfiles/`

!!! Question 19

19. On ServerB, write a script “aspellcheck.sh” that can be used for spell checking by using aspell, to check whether a word is in an aspell-en dictionary or not.
    - aspell is a deprecated package in redhat 9

    ```
    - `vi ~/aspellcheck.sh`
    ```

    File editor:

```
#!/bin/bash
echo $1 > spellcheck.txt
hunspell -d en_US spellcheck.txt
```

- - `chmod a+x ~/spellcheck.sh`

Question 20

20. On ServerB, all new users should have a file name “YouDidIt” in their home folder after account creation.
    - `touch /etc/skel/YouDidIt`

Question 21

21. On ServerB, as root create a cron job that deletes empty directories from the “/tmp” directory at 10 pm on weekends (Saturday and Sunday).
    - `crontab -e`
        - Add the line: `00 22 * * 6-7 find /tmp -type d -empty -delete`

Question 22

22. On ServerB, create an archive file “/root/local.tgz” for “/usr/local”. It should be compressed by gzip.
    - `tar czvf /root/local.tgz /usr/local`

Question 23

23. On ServerB, use /dev/sdb to create a 2G swap partition which takes effect automatically at boot start.
    - `free -h`
    - `lsblk`
    - `fdisk /dev/sdb`
        - `p` `n` `p` `3` `Enter` `+2G` `p` `l` `t` `3` `82` `p` `w`
    - `lsblk`
    - `mkswap /dev/sdb3`
    - `blkid`
    - `vi /etc/fstab`
        - Add the line: `UUID=... swap swap defaults 0 0`

- `swapon /dev/sdb3`
- `free -h`

Question 24

24. Set up SSH Password-less root login in ServerA.
    - `ssh-key-gen`
    - `ssh-copy-id root@192.168.1.4`

Question 25

25. Limit SSH access to Sam on ServerB.

    Note that
    The phrase "Limit SSH access to Sam on ServerB" means that you should configure the SSH (Secure Shell) service on the system named ServerB in such a way that only a user named Sam is allowed to log in remotely via SSH.
    - `vi /etc/ssh/sshd_config`
        - Add the line: `AllowUsers Sam`
    - `useradd Sam`
    - `passwd Sam`
    - `systemctl restart sshd`

Question 26

26. On ServerB, set the limit for the number of SSH login attempts to three.
    - `vi /etc/ssh/sshd_config`
        - Change line to: `MaxAuthTries 3`
        - Remember that running the `ssh` command counts as 1 auth attempt
    - `systemctl restart sshd`

Question 27

27. On ServerB, set SELinux to “permissive” mode.
    - `getenforce`
    - `setenforce 0`

- OR
    - `vi /etc/selinux/config`
        - Change line to: `SELINUX=permissive`

Question 28

28. On ServerB, do the following:
    1. Install container-tools.

2. Run a WordPress container in detached mode with the name "mywordpress" using podman. Mount the “/home/wordpress/var/www/html/” directory in the host to the “/var/www/html” directory in the podman container. Ensure that the bind-mounted volume is private. Map TCP port 80 in the container to port 80 on the host.
   - `dnf install container-tools -y`
   - `podman search wordpress`
   - `podman pull docker.io/library/wordpress`
   - `podman tag docker.io/library/wordpress localhost/wordpress`
   - `systemctl stop httpd` (In case http is using port 80)
   - `mkdir -p /home/wordpress/var/www/html`
   - `podman run --name mywordpress -d -v /home/wordpress/var/www/html/:/var/www/html:Z -p 80:80 localhost/wordpress`
   - `podman ps`
   - `firewall-cmd --list-all`
   - `firewall-cmd --add-port=80/tcp --permanent`
   - `firewall-cmd --reload`
   - `firewall-cmd --list-all`
   - `curl http:/localhost:80` (Or open the browser and verify)

Question 29

29. On ServerB, add a new environment variable “VAR” with the value “RHCSA Prac Six” which will be available for remote login sessions for all users.
    - `vi /etc/bashrc`
      - Add the line: `export VAR='RHCSA Prac Six'`
    - `source /etc/bashrc`
    - `echo $VAR`

Question 30

30. Block the FTP service on ServerB.
    - `firewall-cmd --list-all`
    - `firewall-cmd --remove-service=ftp --permanent`
    - `firewall-cmd --reload`
    - `firewall-cmd --list-all`

- OR
  - `firewall-cmd --add-rich-rule='rule family="ipv4" service name="ftp" reject' --permanent`
  - `firewall-cmd --reload`
  - `firewall-cmd --list-all`

Question 31

31. On ServerB, configure “logrotate” to follow the following specifications:
    - Rotate log files weekly.
    - Keep 2 weeks worth of backlogs.
    - Create new log files after rotating old ones.
    - Compress log files.

```
- ==`vi /etc/logrotate.conf`==
```

File editor:

```
# rotate log files weekly
weekly

# keep 4 weeks worth of baklogs
rotate 2

# create new (empty) log files after rotating old ones
create

...

# uncomment this if oyu want your log files compressed
compress

...
```

- - `systemctl restart logrotate`

Question 32

31. On ServerB, configure the system to log all daemon messages to “/var/log/mylog.log” file.
    - `echo "daemon.* /var/log/mylog.log" >> /etc/rsyslog.conf`
    - `systemctl restart rsyslog`

Question 33

33. On ServerB, configure the bash history to be able to store the last 1000 used commands.
    - `vi /etc/bashrc`
        - Add the line: `export HISTSIZE=1000`
    - `source /etc/bashrc`
    - `echo $HISTSIZE`

Question 34

34. On ServerB, install an FTP server (vsftpd) on your server. Make sure it starts automatically after reboot, then configure it to allow local users to access the remote FTP server and to block anonymous users.
    FTP Ports:
    - Port 21/tcp to allow access to FTP services from external systems.
    - Ports 20000-20100/tcp to allow passive communication with the FTP server.
    - `dnf install ftp vsftpd -y`
    - `systemctl enable vsftpd --now`
    - `systemctl status vsftpd`
    - `firewall-cmd --list-all`
    - `firewall-cmd --add-port=21/tcp --permanent`

- `firewall-cmd --add-port=20000-20100/tcp --permanent`
- `firewall-cmd --reload`
- `firewall-cmd --list-all`
- `vi /etc/vsftpd/vsftpd.conf`
  - Change line to: `anonymous_enable=NO`
  - Change line to: `local_enable=YES`
- `systemctl restart vsftpd`

Question 35

35. On ServerB, create a Stratis Pool using /dev/sde. Then mount it persistently on the “/stratis” directory.
    - `dnf install stratisd stratis-cli -y`
    - `systemctl enable stratisd --now`
    - `systemctl status stratisd`
    - `lsblk`
    - `blkid -p /dev/sde`
    - `wipefs -a /dev/sde`
    - `stratis pool create mypool /dev/sde`
    - `stratis pool list`
    - `stratis fs create mypool filesystem`
    - `stratis fs list`
    - `lsblk`
    - `blkid -p /dev/stratis/mypool/filesystem`
    - `mkdir /stratis`
    - `vi /etc/fstab`
      - Add the line: `UUID=... /stratis xfs defaults,x-systemd.requires=stratisd.service 0 0`
    - `systemctl daemon-reload`
    - `mount /stratis`

Question 36

36. On ServerB, list installed kernels and save them in the “/all_kernels” file.
    - `grubby --info=ALL | grep kernel > /all_kernels`
    - `cat /all_kernels`

Question 37

37. On ServerB, set the default kernel to index 1.
    - `grubby --info=ALL | grep -E "kernel|index"`
    - `grubby --set-default-index=1`
    - `grubby --default-index`

Question 38

38. On ServerB, remove the "quiet" argument from the default kernel boot entries.

- `cd /boot`
- `ls`
- `grubby --update-kernel=/boot/vmlinuz-5.14.0-... --remove-args="quiet"`
- `grubby --update-kernel=/boot/vmlinuz-0-rescue-... --remove-args="quiet"`
- `grubby --info=ALL | grep args`
- `grub2-mkconfig -o /etc/grub2.cfg`

- OR
  - `grubby --update-kernel=ALL --remove-args="quiet"`
  - `grubby --info=ALL | grep args`
  - `grub2-mkconfig -o /boot/grub2/grub.cfg`

Question 39

39. On ServerB, find All Files in /etc (not subdirectories) that contain text "ntp" (ignore case), and append them to the file "/ntp_files".
    - `ls -l /etc | grep -i ntp >> /ntp_files`

- OR
  - `grep -rli ntp /etc >> /ntp_files`

Question 40

40. On ServerB, schedule the backup script "/etc/scripts/backup.sh" to run every 30 minutes.

    Required
    To resolve this task, you must create the `/etc/scripts/backup.sh` file if the file does not exist.
    - `mkdir /etc/scripts`
    - `touch /etc/scripts/backup.sh`
    - `chmod a+x /etc/scripts/backup.sh`
    - `crontab -e`
      - Add the line: `*/30 * * * * /etc/scripts/backup.sh`

Question 41

41. On ServerB, create a script named "locate.sh" placed in "/usr/local/bin/" that is used to find all files larger than 30KB, but less than 50KB and have SUID permission, then send the filenames to the file "/root/locatedfiles".

    ```
    - `vi /usr/local/bin/locate.sh`
    ```

    File editor:

```
#!/bin/bash
find / -size +30K -size -50K -perm -u=s > /root/locatedfiles
```

- - `chmod a+x /usr/local/bin/locate.sh`

- `/usr/local/bin/locate.sh`
- `cat root/locatedfiles`

Question 42

42. Manually boot ServerA into the multi-user target.
    - `systemctl isolate multi-user.target`
    - `systemctl status multi-user.target`

Question 43

43. On ServerB, allow incoming SSH connections from the 192.168.1.13/24 network and deny all other incoming connections.
    - `firewall-cmd --list-all`
    - `firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.1.13/24" service name="ssh" accept'`
    - `firewall-cmd --add-rich-rule='rule family="ipv4" source address="0.0.0.0/24" service name="ssh" reject'`
    - `firewall-cmd --list-all`
    - `firewall-cmd --runtime-to-permanent`