# Appendix C

## Solutions to RHCSA Sample Exam 2

The questions in the RHCSA Sample Exam 2 will help measure your understanding of the material covered in this book. As indicated in the introduction, you should be capable of completing the RHCSA exam in 3 hours. However, we have capped the time for this lab at 2.5 hours to accustom you to working under time constraints.

The RHCSA exam follows a "closed book" format. Nevertheless, you are permitted to refer to any documentation available on the Red Hat Enterprise Linux computer. Although test centers permit note-taking, these notes cannot be taken out of the examination room.

In the majority of cases, there isn't a single solution or method to resolve a problem or install a service. With the plethora of options available in Linux, it is impossible to cover every potential scenario.

For the forthcoming exercises, avoid using a production computer. Even a minor error in any of these exercises could render Linux unbootable. If you cannot recover using the steps provided in these exercises, you might need to reinstall Red Hat Enterprise Linux. Consequently, you may not be able to recover any data saved on the local system.

Red Hat conducts its exams electronically, which is why the exams in this book can be accessed from the McGraw Hill companion website. This exam, named RHCSAsampleexam2, is available in PDF format. For instructions on setting up RHEL 9 as a suitable system for a practice exam, please refer to Appendix A.

# RHCSA Sample Exam 2 Discussion

In this discussion, we'll describe briefly one way to meet the requirements listed for the RHCSA Sample Exam 2.

1. To complete this task, review Exercise 5-2, "Recover the Root Password," in Chapter 5.
2. Assuming that the network interface is named eth0, execute the following commands:

```
# nmcli con mod eth0 ipv4.method auto
# nmcli con mod eth0 ipv4.gateway ""
# nmcli con mod eth0 ipv4.address ""
# nmcli con down eth0
# nmcli con up eth0
# hostnamectl set-hostname server1.example.com
```

3. To complete this task, review Exercise 4-2, "Subscribe a System to the Red Hat Subscription Management," in Chapter 4. Then, install the tmux RPM package with the following command:

```
# dnf install tmux
```

4. Use the **parted** command to create a new partition. Assume that your hard drive is /dev/vda, the new partition is number 3, and there is some free space starting at about 19GB. Start the **parted** utility with **parted /dev/vda** and type

```
(parted) unit mib
(parted) print
(parted) mkpart primary 19000MiB 19500MiB
(parted) quit
```

5. Run the following commands to format the filesystem and create the mount point:

```
# mkfs.xfs /dev/vda3
# mkdir /sysadmins
```

Add an entry to the /etc/fstab file. You will use the UUID (Universally Unique Identifier) of the partition for this, which you can obtain by running the **blkid** command as follows:

```
# blkid /dev/vda3
```

Then, add the following line to /etc/fstab:

```
UUID=<substitute with UUID value>   /sysadmins   xfs   defaults   0 0
```

And mount the filesystem:

```
# mount /sysadmins
```

6. Use the **parted** command to create a new partition. Assume that your hard drive is /dev/vda, and the new partition is number 4. Start the **parted** utility and type

```
mkpart primary 19500MiB 19600MiB
set 4 swap on
quit
```

7. Format the new partition as swap:

```
# mkswap /dev/vda4
```

Find the UUID of the partition:

```
# blkid /dev/vda4
```

Then, add the following line to /etc/fstab:

```
UUID=<substitute with UUID value>   none swap   defaults   0 0
```

And mount the filesystem:

```
# swapon /dev/vda4
```

8. The following command shows one method to complete this task:

```
# find /etc -type f -exec grep -l redhat {} \;↵
>/root/etc-redhat.txt
```

9. New local users should be listed in /etc/passwd and /etc/shadow. To specifically deny regular users access to a directory, you can create a dedicated group for this purpose, for example "sysadmins". You should be able to confirm that users bill and richard don't have access to the /sysadmins directory by trying to list its contents or creating a file in it.

To complete the task, run the following commands:

```
# useradd linus
# useradd richard
# useradd mark
# useradd bill
# echo "redhat123" | passwd --stdin linus
# echo "redhat123" | passwd --stdin richard
# echo "redhat123" | passwd --stdin mark
# echo "redhat123" | passwd --stdin bill
# groupadd sysadmins
# usermod -aG sysadmins linus
# usermod -aG sysadmins mark
# mkdir /sysadmins
# chgrp sysadmins /sysadmins
# chmod 770 /sysadmins
```

10. Install the autofs and nfs-utils packages:

    ```
    # dnf install autofs nfs-utils
    # systemctl enable autofs --now
    ```

    Then, add the following line to /etc/auto.misc:

    ```
    dvd -fstype=iso9660,ro,nosuid,nodev :/dev/cdrom
    ```

    To confirm your change, add an ISO file to the virtual drive on the virtual machine. Then, run the **ls /misc/dvd** command, and the automounter should mount the DVD and provide file information on that drive. This should be an easy configuration, based on a slight change to the default /etc/auto.misc file. Of course, you'll need to make sure the autofs service runs after a reboot, which you can confirm with the **systemctl is-enabled autofs** command.

11. To set the system to boot into the multi-user target by default, use the following command:

    ```
    # systemctl set-default multi-user.target
    ```

    You can verify that the default target has been set correctly with this command:

    ```
    # systemctl get-default
    ```

12. Open the file /etc/chrony.conf and locate any lines that start with server or pool. Comment those lines out by adding a # character at the beginning of each line. Then, add a new line to specify time.google.com as the server:

    ```
    pool time.google.com iburst
    ```

    Restart the **chronyd** daemon to apply the changes:

    ```
    # systemctl restart chronyd
    ```

    To verify the current NTP sources, run

    ```
    # chronyc sources
    ```

13. Open the /etc/selinux/config file. Locate the line that starts with **SELINUX=**. This line specifies the SELinux mode. Change it to **SELINUX=permissive**, save the file, and reboot the system. To verify that SELinux is set in permissive mode, run the **sestatus** command.

14. Make sure the NFS client utilities are installed. You can do so with the following command:

    ```
    # dnf install nfs-utils
    ```

Create the directory where the NFS share will be mounted:

```
# mkdir /mnt/nfs
```

Then, add the following line to /etc/fstab (substitute for the IP address of tester1.example.com):

```
<ip_of_tester1>:/exports/nfsshare  /mnt/nfs  nfs  defaults  0 0
```

To mount the filesystem, run

```
# mount /mnt/nfs
```

15. As user mark on server1.example.com, generate an RSA SSH key pair with a key length of 4096 bits:

```
$ ssh-keygen -t rsa -b 4096
```

Now, create user mike on tester1.example.com:

```
# useradd mike
# echo "changeme" | passwd --stdin mike
```

Then, on server1.example.com, copy the public key to the destination server tester1.example.com. You can do this using the **ssh-copy-id** command (substitute for the IP address of tester1.example.com):

```
$ ssh-copy-id mike@<ip_of_tester1
```

You will be prompted to enter user mike's password for tester1.example.com to allow the copy operation. Now, user mark from server1.example.com should be able to SSH into tester1.example.com as user mike using key-based authentication. When you initiate the SSH connection, you'll be prompted to enter the passphrase for the key.

16. First, make sure that the tuned RPM is installed and the service is running. If not, install the package, start the service, and enable it to start at boot:

```
# dnf install tuned
# systemctl start tuned
# systemctl enable tuned
```

Now, to activate the virtual-guest profile, use the **tuned-adm** tool:

```
# tuned-adm profile virtual-guest
```

To verify the active profile, you can use the following command:

```
# tuned-adm active
```

17. As user bill, create a Containerfile with the following content:

    ```
    # Use the Red Hat UBI 9 image as the base
    FROM registry.access.redhat.com/ubi9/ubi:latest
    # Execute the "sleep 1d" command
    CMD ["sleep", "1d"]
    ```

    Use the following command to build the image:

    ```
    $ podman build -t ubi-test .
    ```

18. Just like with all Red Hat exams, it's essential for your modifications to endure a system reboot. Therefore, reboot the system and verify that your configurations remain fully functional.