Appendix C

Sample Exam 2: RHCSA

The following questions will help measure your understanding of the material presented in this book. As discussed in the introduction, you should be prepared to complete the RHCSA exam in 2.5 hours.

The RHCSA exam is “closed book.” However, you are allowed to use any documentation that can be found on the Red Hat Enterprise Linux computer. While test facilities allow you to make notes, you won’t be allowed to take these notes from the testing room.

The RHCSA is entirely separate from the RHCE. Although both exams cover some of the same services, the objectives for those services are different.

In most cases, there is no one solution, no single method to solve a problem or install a service. There is a nearly infinite number of options with Linux, so we can't cover all possible scenarios.

Even for the following exercises, *do not use a production computer*. A small error in some or all of these exercises may make Linux unbootable. If you're unable to recover from the steps documented in these exercises, you may need to reinstall Red Hat Enterprise Linux. Saving any data that you have on the local system may then not be possible.

Red Hat presents its exams electronically. For that reason, the exams in this book are available from the companion DVD, in the Exams/ subdirectory. This exam is in the file named RHCSAsampleexam2 and is available in .txt, .doc, and .html formats. For details on how to set up RHEL 7 as a system suitable for a practice exam, refer to Appendix A. Be very sure to set up the repository configured in Chapter 1, Lab 2.

Don't turn the page until you're finished with the sample exam!

RHCSA Sample Exam 2 Discussion

In this discussion, we'll describe one way to check your work to meet the requirements listed for the Sample 2 RHCSA exam.

1. If the virtualization software is installed on the local system, you'll have access to the Virtual Machine Manager in the GUI, or at least the **virt-install** and **virsh** commands from the command line.
2. If the newly Kickstarted installation is successful, you should be able to access the new outsider2.example.org system, either via ssh or with the Virtual Machine Manager.
3. Anyone with access to the administrative account on the VM can review ssh-based logins in the /var/log/secure file. It's an easy way to verify that you've used the **ssh** command to connect to the new system. If you don't know how to recover a root password, review Exercise 5-2.
4. All partitions (the new 500MB partition, additional swap space) should be shown in the output to the **fdisk -l** command.
5. When properly configured, the new filesystem should be shown in the output to the **mount** command, marked as "type xfs."
6. When additional swap space is created, it should be shown in the contents of the /proc/swaps file. Alternatively, the total amount of swap space should be shown in the output to the **free** command.
7. Run the **blkid** command to retrieve the UUID of the new volumes to be set in /etc/fstab. The type of the filesystem must be specified as swap in the /etc/fstab file. Here's an example:

   ```
   UUID=a110ef54-caed-42b2-a5bb-e3086792d168 swap swap defaults 0 0
   ```

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

   ```
   # grep -rl redhat /etc/* >/root/etc-redhat.txt 2>/dev/null
   ```

   Another method is listed next:

   ```
   # find /etc -type f -exec grep -l redhat {} \;↵
   >/root/etc-redhat.txt 2>/dev/null
   ```

9. New local users should be listed in /etc/passwd and/etc/shadow. To specifically deny regular users access to a directory, it's easiest to use ACLs. You should be able to confirm that users bill and richard don't have access to the /cooks directory with the **getfacl /cooks** command. Try to create a file as user bill or richard with the **touch** command.

   ```
   # getfacl /cooks
   getfacl: removing leading '/' from absolute path names
   # file: cooks
   # owner: root
   # group: root
   user::rwx
   user:bill:---
   user:richard:---
   group::r-x
   mask::rwx
   other::rwx
   ```

10. To confirm, you should be able to insert a DVD into the appropriate drive. (Alternatively, you can set up an ISO file on a virtual machine.) Then when you run the **ls /misc/dvd** command, the automounter will 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. If unsure, review Chapter 6, Certification Objective 6.06. Of course, you'll need to make sure the autofs service runs after a reboot, which can be confirmed with the **systemctl is-enabled autofs** command.
11. When new kernels are installed, they should include a new stanza in the bootloader configuration file, /boot/grub2/grub.conf. The default stanza is based on the **saved_entry** directive in the /boot/grub2/grubenv file; just remember, **saved_entry=0** points to the first stanza, **saved_entry=1** points to the second stanza, and so on. Use the **grub2-set-default** command to boot a different default kernel.
12. Default targets are configured with the **systemctl set-default** command.
13. Edit the /etc/ntp.conf file. The **server** directive in that file should point to the desired system (in this case, the physical host). Of course, a test on that system with the **ntpq -p** command won't work unless the physical host is configured as an NTP server. In a real-world configuration, that second host would be an actual NTP server. Once again, you'll need to make sure the ntpd service runs after a reboot, which can be confirmed with the **systemctl is-enabled ntpd** command.
14. To make sure SELinux is set in permissive mode, run the **sestatus** command.