Appendix B

Sample Exam 1: 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 RHCSAsampleexam1 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 1 Discussion

In this discussion, we'll describe one way to check your work to meet the requirements listed for the Sample 1 RHCSA exam.

1. One way to see if SELinux is set in enforcing mode is to run the **sestatus** command.
2. 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.
3. If successful, you should be able to access the new server2.example.com system, via ssh or with the Virtual Machine Manager.
4. One way to set the noted system to start automatically the next time the host is booted is with the **virsh autostart server2.example.com** command. One way to confirm this is in the output to the **virsh dominfo server2.example.com** command.
5. If you don't know how to recover a root password, review Exercise 5-2.
6. To review current volume groups, run the **vgdisplay** command. Check the PE size. To list all logical volumes, run the **lvdisplay** command. The size of the new volume should be 32 logical extents, equivalent to 256MB.
7. To make sure that volume is automatically mounted the next time the system is booted, it should be configured in /etc/fstab to the appropriate format, with the UUID associated with the volume, as provided by the **blkid** command. Here's an example:

   ```
   UUID=d055418f-1ff6-46bf-8476-b391e82a6f51 /project xfs defaults 1 2
   ```

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

   ```
   # find /etc -type f -name "*.conf" >/root/configfiles.txt 2>/dev/null
   ```

9. Run the **file /tmp/etc.tar.bz2** command to confirm that the file you have created is bzip-compressed. Uncompress the archive to verify its content, or check its content with the following command:

   ```
   # cat /tmp/etc.tar.bz2 | bunzip2 | tar -t
   ```

10. The /home/friends directory should be owned by the group friends. As long as users donna and mike are not part of that group, and other users don't have permissions (or ACLs) on that directory, access should be limited to members of the friends group. The directory should also have SGID permissions:

    ```
    # ls -ld /home/friends
    drwxrws---. 2 root friends 6 Nov 18 10:54 /home/friends
    # getent group friends
    friends:x:2000:nancy,randy
    ```

11. If you've modified user mike's account to make his account expire in seven days, the right expiration date should appear in the output to the **chage -l mike** command.
12. There are a number of ways to set up a cron job; it could be configured in the /etc/cron.monthly directory or as a cron job for the user root or mike with the **crontab -u mike -e** command. In any of these cases, the command would be associated with an appropriate timestamp, with a line such as this:

```
50 3 2 * * /bin/find /home/mike/tmp -type f -exec /bin/rm {} \;
```

13. Run the **getfacl /home/mike/project.test** command. If user donna has read permissions in the ACLs, you'll see it in the output to that command. You should also set an ACL on the /home/mike directory and grant user donna the execute permission in order to access files within the directory.
14. Run the **authconfig-gtk** command to review the current settings. "Use LDAP" must be enabled in the User Information settings, along with "Use LDAP Authentication." The server URL should be set to ldap://192.168.122.1, with TLS enabled.