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. While 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 are a nearly infinite number of options with Linux, so I can't cover all possible scenarios.

Even for these 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 CD, 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 6 as a system suitable for a practice exam, refer to Appendix A.

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

RHCSA Sample Exam 2

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

1. If VM 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.
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 ext4 format should be shown in the output to the **mount** command, and permanent settings (including the acl option, the /cooks directory, and corresponding UUIDs) shown in the /etc/fstab file.
6. When additional swap space is implemented, 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 **top** command.
7. New local users should be documented in /etc/passwd and/etc/shadow.
8. 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.
9. 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. Of course, you'll need to make sure the autofs service runs after a reboot, which can be confirmed with an **chkconfig --list autofs** command.
10. When new kernels are installed, they should include a new stanza in the bootloader configuration file, /boot/grub/grub.conf. The default stanza is

based on the **default** directive; just remember, **default=0** points to the first stanza, **default=1** points to the second stanza, and so on.

11. Default runlevels are still configured in the /etc/inittab file.
12. If successful, you should be able to retain (or restore) the same SELinux contexts as /var/ftp with the **restorecon /ftp** command. That requires appropriate entries in the file_contexts.local file, in the /etc/selinux/targeted/contexts/files directory, based on the appropriate **semanage fcontext** command.
13. On an NTP client configured to point to another system, look at 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 also an NTP server. On an actual exam (or 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 an **chkconfig --list ntpd** command.
14. To make sure SELinux is set in permissive mode, run the **sestatus** command.