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. 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 RHCSAsampleexam1, 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 1 Discussion

In this discussion, I'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 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.
3. If successful, you should be able to access the new server2.example.com system, either 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 is in the output to the **virsh dominfo server2.example.com** command.
5. To review current logical volumes, run the **lvs** command.
6. Make sure the volume is encrypted. Did you run the **cryptsetup** command on the volume?
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 encrypted volume, as defined by the **blkid** command.
8. The /home/angels directory should be owned by the group angels. 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 angels group. The directory should also have SGID permissions.
9. 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.
10. 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 in the /var/spool/cron directory. In any of these cases, the delete command would be associated with an appropriate time stamp, with a line such as:

```
50 3 2 * * /bin/rm /home/mike/*
```

11. Permanently configured ACLs are associated with the acl option on the appropriate volume in the /etc/fstab configuration file. Volumes mounted with the acl option should be revealed in the output to the **mount** command.
12. 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.
13. For a GRUB stanza to point to runlevel 1, that number must be included in the command associated with the **kernel** directive.
14. A change to the root password, where that password isn't already known, is intended to make you boot into single-user mode.
15. The process for installing an Apache Web server is straightforward. It can be verified with the **rpm -q httpd** command.
16. But you need to make sure the server starts automatically the next time the system is booted, something that can be checked with the **chkconfig --list httpd** command.
17. To make that server accessible to all systems over a network, at least port 80 should be open in the **iptables**-based firewall. If a local system is on IP address 192.168.122.51, that can be confirmed from a remote system with the **nmap 192.168.122.51** command. Of course, if you revise the default Apache server port, the changes required to the firewall must also comply.