Appendix E

Sample Exam 4: RHCE Sample Exam 2

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 RHCE exam in 3.5 hours.

Like the RHCSA, the RHCE 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.

Although the RHCE exam is entirely separate from the RHCSA, you need to pass both exams to receive the RHCE certificate. Nevertheless, you can take the RHCE exam first. 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 is a nearly infinite number of options with Linux, so we 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 DVD, in the Exams/ subdirectory. This exam is in the file named RHCEsampleexam2 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!

RHCE 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 RHCE exam. Since there is no one way to set up a Red Hat Enterprise Linux configuration, there is no one right answer for the listed requirements. However, there are some general things to remember. You need to make sure your changes work after a reboot. For the RHCE, you'll need to make sure that the services you set up are configured to start automatically at boot.

1. This task is essentially identical to Exercises 12-5 and 12-6. To verify the configuration, ensure that Kerberos principals exist on the KDC for each user. After you open an SSH session on server1, the **klist** command should confirm that a TGT has been granted. In case of issues, review the configuration. Based on the question, the client should include the following directives in /etc/krb5.conf:

   ```
   default_realm = EXAMPLE.COM
   ```

   In addition, the kdc and admin_server directives in the /etc/krb5.con file should be set to the FQDN of the physical host system.
2. The first part of this task requires the following configuration line in /etc/exports:

   ```
   /nfsshare tester1.example.com(rw)
   ```

   The configuration of an NFS share secured with Kerberos is explained in Exercises 16-2 and 16-3. Verify that you have created and installed Kerberos host and service principals for all your machines. On the server, the nfs-server and nfs-secure-server services must be running. The NFS share must be exported with the **sec=krb5p** option.
3. This exercise is the continuation of the previous task. If the client can automatically mount the NFS share at boot with the **sec=krb5p** option, you have successfully completed this task. If you face any issues, check that the nfs-secure service is enabled on the client and review your firewall rules. Run the **mount** command in verbose mode (**-v**) and analyze the output and the logs for error messages.
4. If successful, you should see the contents of the noted index.html files for each website. You should also change the default SELinux context of the /web directory to match that of the /var/www/html directory. Review Chapter 14, Certification Objective 14.04, for more information on secure virtual hosts.
5. If you are successful, users elizabeth and fred, and no others, will have access to the cubs subdirectory of the main directory. Both users will have access only from systems on the local network. If your configuration does not work as expected, review your setup. You must have a **<Directory>** block container for the cubs subdirectory in the Apache configuration files, with **AuthType Basic** and **Require user** directives. You will also need an **AuthUserFile** line pointing to a password file. You can restrict access to the local network with an **Allow from** directive.

6. The CGI application should be accessible from the following URL:
   http://test1.example.com/cgi-bin/good.pl
   When you navigate to that URL, the browser should print the string "Good Job!"
7. If you use BIND, the default named.conf configuration file is itself sufficient for a caching-only DNS server. To that file, you'll need to add a **forwarders** directive, with the IP address of the physical host system, which presumably has a DNS server.
8. Configure Postfix and review your configuration with the **postconf -n** command. At a minimum, you need to configure the **myorigin**, **mydestination**, **local_transport**, and **relayhost** directives. Test the configuration with an e-mail client such as mutt. The server should accept e-mails from the local system only and deliver them to your physical host. Verify in /var/log/maillog that this is the case.
9. When user mike attempts to connect from a given client, the system should prompt for and accept the passphrase defined in the exam question: **Linux rocks, Windows does not.** (Note that the passphrase includes a comma and period.) SSH key-based authentication is a requirement for both the RHCSA and RHCE exams and was covered in in Chapter 4, Certification Objective 4.04.
10. When masquerading is configured, connections from internal systems in the 192.168.122.0/24 network such as server1.example.com to outsider1.example.net appear as if they come from the physical host system. That can be confirmed by attempting a SSH connection and looking at log messages in /var/log/secure.
11. If the configuration works, you should still have IP connectivity after disabling one of the interfaces with the **ifdown** command. Verify that round-robin mode is in use with the **cat /proc/net/bonding/bond0** command (if you configured bonding) or with the **teamdctl team state** command (if you configured teaming). For more information on interface teaming and bonding, review Chapter 12, Certification Objective 12.06.
12. Users with an account on the Samba server should be able to connect to their home directories on that server. However, the files on that directory won't be accessible unless the samba_enable_home_dirs boolean is enabled.
13. Peers on an NTP server can be enabled in the /etc/ntp.conf file, in place of the **server** directive. Just remember, NTP communicates over UDP port 123. One way to check if UDP port 123 is open is with the following command: **nmap -sU server1 -p 123**.
14. To avoid responding to the **ping** command, which works over IPv4, the **icmp_echo_ignore_all** option must be active. You can set that up permanently in the /etc/sysctl.conf file with the **net.ipv4.icmp_echo_ignore_all = 1** directive.