Appendix D

Sample Exam 3: RHCE Sample Exam 1

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 RHCEsampleexam1 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 1 Discussion

In this discussion, we'll describe one way to check your work to meet the requirements listed for the Sample 1 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. The first task should be straightforward. Users katie and dickens should have accounts on the SSH server. While it's possible to limit user access to SSH via TCP Wrappers, the most straightforward way to do so is with the following directive in the main SSH server configuration file:

   ```
   AllowUsers katie
   ```

   Of course, the "proof of the pudding" is the ability for user katie to log in from a remote system on the local network and for user dickens to be refused such access. In addition, limited access to the local network requires an appropriate limit via a zone-based firewall rule, or an appropriate line in the TCP Wrappers configuration files, /etc/hosts.allow and /etc/hosts.deny.
2. The Samba server will be configured with two different shared directories. The system can be configured with the samba_export_all_rw SELinux boolean, or alternatively, the directories should be set with the samba_share_t type label. In addition, the most straightforward way to limit access to the given users is with the **allow users** directive in the smb.conf configuration file in the appropriate stanzas. The given users should exist in the separate Samba password database. Of course, success is based on the ability of users dickens, tim, and stephanie to access the given directories from a remote system.
3. NTP servers are limited to the local system by default. Expanding access to the local network requires a change to the /etc/ntp.conf file, in the **restrict** directive, as well as appropriate open ports in the firewall. You can test the connection remotely with the **ntpdate *ntpserver*** command. (Of course, you're welcome to substitute the IP address for the hostname of the NTP server.) Remember, NTP communicates over UDP port 123.
4. Although other methods are available, you can limit access in the main NFS configuration file (/etc/exports) to a single host, with a directive such as the following:

   ```
   /home maui.example.com(rw)
   ```

You should substitute the hostname or IP address of your physical exam system. In addition, you may run into different requirements, such as read-only (ro), no root access (root_squash), and more. Access should be confirmed from the physical host system by mounting the shared NFS directory.

5. The most straightforward way to configure a secure virtual website is with the help of the standard configuration defined in the ssl.conf file in the /etc/httpd/conf.d directory. If successful, you'll be able to access the secure websites https://shost1.example.com and https://shost2.example.com. Since these certificates aren't from an official authority, you should not be concerned about the "invalid security certificate" message that appears in a browser, assuming the SSL key names are shown in the message.
6. Add the https service to the default zone on the local zone-based firewall of server.example.com. To limit HTTP access from outstider1.example.net, you can set up a rich rule. Alternatively, add the IP address of outsider1 to the drop zone on the firewall. Before testing, ensure that DNS resolution for the hostnames shost1.example.com and shost2.example.com works by adding the IP and host entries to the /etc/hosts files of every machine.
7. The typical location for a daily cron job is the /etc/cron.d directory. The backup.sh script must be run from the local directory where the backup files need to be saved. Hence, you should change to the /tmp directory before running the script. The cron line should look like this:

```
0 2 * * * root (cd /tmp; /usr/local/bin/backup.sh /home)
```

8. To configure IP forwarding for both IPv4 and IPv6 addressing, you'll need to add the following directives in /etc/sysctl.conf:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

9. Success on this task can be verified by "pinging" the two IPv6 addresses from the two hosts, with the commands **ping6 2001:db8:1::1/64** and **ping6 2001:db8:1::2/64**.
10. Use the **targetcli** shell to set up the iSCSI target. Upon completion, the **targetcli ls** command should display all the required configuration parameters. Review Chapter 13, Certification Objective 13.06, for more information on how to use the **targetcli** shell.
11. On the client, run the **iscsiadm** command in discovery database mode to see the remote target. If no targets are displayed, review the configuration, including the iSCSI access list, the IQN names, and firewall rules. Ensure that the iscsi and target services are running on the client machine and the storage server, respectively. If the discovery phase is successful, log in to the target and create a filesystem. You would need an entry in /etc/fstab to automatically mount the volume at boot.

12. The default time period when the system accounting tool is run is 10 minutes, as shown in the default /etc/cron.d/sysstat file. It's easy to change that to one minute in the noted file.
13. Connect with the **mysql -u root** command to the database and issue the following commands:

    ```
    USE exam;
    SELECT * from mark;
    ```

    The SELECT query should return the three records listed in the exercise.
14. If successful, you should be able to log in to the MariaDB database by running **mysql -u examuser -p** and typing **pass123**. The user must have full access to the exam database, which you can confirm with the **SHOW GRANTS** command. The root user must not be able to access MariaDB without a password. You can confirm that this is the case with the **mysql -u root** command.