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 2.0 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.

While 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 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 RHCEsampleexam1, 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.

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.

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

RHCE 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 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. But 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 that you set up are active at the appropriate runlevels. For example, if you're configuring Apache, it should be active for at least runlevels 3 and 5.

1. The first task should be straightforward. Users katie and dickens should have accounts on the SSH server (or possibly an LDAP server for the network). 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 an **iptables**-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 the directories can 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 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. Since there are no host limits in the vsFTP configuration file, access limits require appropriate rules in iptables-based firewalls and/or TCP Wrappers configuration files. Success is based on anonymous access from the given server1.example.com and physical host systems (along with access prohibited from other systems).
4. 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 **ntpq -p 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.

5. While other methods are available, the straightforward way to limit access in the main NFS configuration file (/etc/exports) can be limited 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, other exams may specify a different set of permissions, 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.
6. The most straightforward way to configure a secure virtual web site is with the help of the standard configuration defined in the ssl.conf file in the /etc/httpd/conf directory. If successful, you'll be able to access the secure web sites https://shost1.example.com and https://shost2.example.com. Since these certificates aren't from an official authority, the "invalid security certificate" message that appears in a browser should not be a problem, assuming the SSL key names are shown in the message.
7. Since a test system is not supposed to have Internet access, you should check access to the caching-only DNS server a bit indirectly with a command like **telnet server1.example.com 53** or **nmap server1.example.com**. Substitute the name or IP address of the DNS server if needed.
8. A daily script can be stored either in the /etc/cron.daily directory or in a user account–based cron configuration file in the /var/spool/cron directory.
9. Success in this step is most straightforward; copy the RPM that you've created to a second system. Install it. If successful, you'll see the README file in the /opt/tcpwrap directory.
10. 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
    ```
11. The time period when the system accounting tool is run is ten minutes, as shown in the default /etc/cron.d/sysstat file. It's easy to change that to five minutes in the noted file.