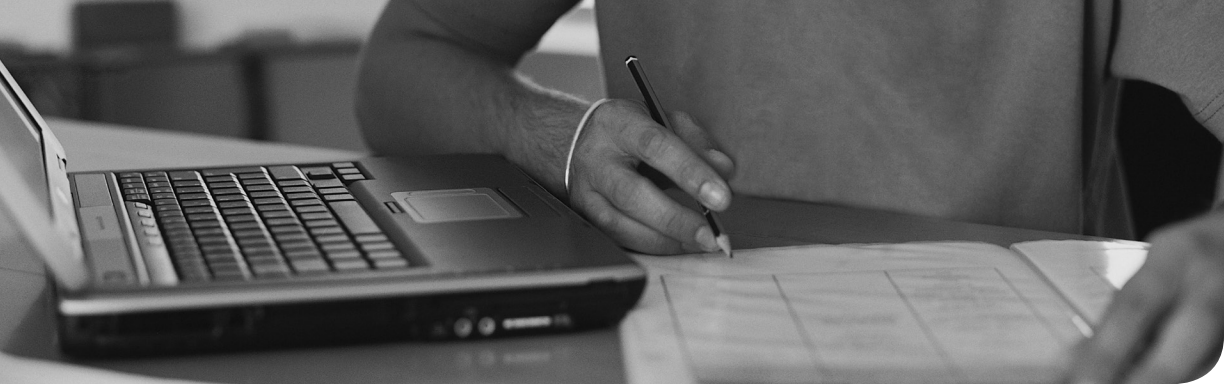

RHCSA Practice Exam B

Note: This exam is also available as a PDF on the book's DVD.

Note: The Premium Edition of this book contains four additional practice exams: two RHCSA and two RHCE. You can find information about upgrading to the Premium Edition in the front of this book.

RHCSA Practice Exam B

This test exam needs the following setup:

- An IPA server that is offering central services such as LDAP and NFS. The setup of such a server is described in Appendix D, "Setting Up Identity Management." Alternatively, the test VMs that are provided on rhatcert.com can be used.
- A cleanly installed virtual machine. Step 1 of this test exam describes how to set up such a virtual machine based on a KVM setup. Notice that the IP addresses that are used in the virtual machines are based on the internal IP addresses in a KVM setup. If you are using another virtualization platform, make sure to change the IP addresses accordingly.
- Unless specifically mentioned, all tasks described below should be performed on the virtual machine.

1. Install an RHEL 7 virtual machine. Use a 12GB LVM volume or disk backend file on the host as the storage backend for the virtual machine. Use the bridged network interface on the host for networking in the virtual machine. (This should normally be done automatically.) Make sure the virtual machine meets the following requirements. All the following tasks are performed on the server unless stated otherwise:
    - 20GB total disk space
    - IP address is 192.168.122.200
    - Set hostname to server1.example.com
    - A 500MB boot partition

- A logical volume for the / file system with a size of 6GB
- A logical volume for swap with a size of 512MB
- Install the Server with GUI installation pattern.

2. Create a partition with a size of 500 MiB. Format this partition with the Ext4 file system and provide it with the label data. Mount this partition persistently through the /etc/fstab file on the /data directory.
3. Use the appropriate command to locate all files on your server that have a size greater than 100MB and store a list of their names in the file /root/bigfile.
4. Create the users lisa and lori. Set their passwords to expire after 90 days.
5. Generate an SSH key pair for the user root. Copy the appropriate key over to your host computer so that you can log in to the host computer without having to enter a password or passphrase.
6. Resize the logical volume that is used by the root file system and add 1 GiB to it. Ensure that the root file system is resized as well.
7. Create the groups profs and students. Make lisa a member of the group profs, and make lori a member of the group students without changing their primary group assignments.
8. Create a directory structure /data/profs and /data/students. Make the appropriate directories fully accessible to the members of their respective groups. In these directories, users should only be able to remove files of which they are the owner, and newly created files should be group owned automatically by the group that is owner of the directory. So if, for example, in /data/profs, user lisa creates a file, it should be group owned by the group profs automatically.
9. Set up file access permissions such that members of the group profs can read all files in the directory /data/students, existing files as well as new files. Also and without changing the umask, in this particular directory the others entity should get no access permissions at all.
10. Configure logging in such a way that all log messages with a priority of warn and higher are written to the /var/log/warnings file.
11. Set up logrotate on the /var/log/warning file such that it will be rotated on a monthly basis. Keep 11 old versions of the file.
12. Set up a firewall such that only the SSH process can be reached on your server.