Labs

During the Red Hat exams, the tasks will be presented electronically. Therefore, this book presents most of the labs electronically as well. For more information, see the "Lab Questions" section toward the end of Chapter 15. Most of the labs for this chapter are straightforward and require very few commands or changes to one or two configuration files.

Lab 1

In this lab, you'll install and set up Samba just for basic operation. If possible, use a system where Samba isn't already installed.

1. Ensure that the appropriate Samba packages are correctly installed. What RPMs did you install and how did you install them?
2. Make sure the samba-client, samba-winbind, and cifs-utils packages are also installed.
3. Make sure any local firewall supports access to the local Samba server. Make sure that the firewall on all clients supports the use of Samba client software.
4. Ensure that the Samba and NetBIOS services are configured to start correctly when you boot Linux.
5. Start Samba and NetBIOS services now. Which **systemctl** command options did you use?
6. Verify that Samba services are running. How did you do this?

Lab 2

During an exam, or perhaps a trip to a remote site where Internet access is not possible, you may need to rely on the Samba documentation available with the installed packages.

1. Open the man page for the Samba configuration file, smb.conf.
2. Make sure that you know how to search for key directives, such as **hosts allow** and **invalid users**.
3. Run **rpm -qd samba samba-client cifs-utils** to list all the Samba documentation files installed in your system.

4. Examine the content of the following man pages: testparm, smbpasswd, samba_selinux, mount.cifs, and cifscreds.

Lab 3

Before starting this lab, it's important to back up the /etc/samba/smb.conf file. Unless you do so, it may be difficult to proceed with additional labs in this chapter.

1. Configure Samba global settings to provide workgroup services to local users. Set the workgroup name to something appropriate for a local organization.
2. Can you limit access to a corporate domain name (such as example.com) through this tool? What do you have to do?
3. Can you prevent access to one specific host or IP address through this tool? Do so for one host on the local network.
4. Save your changes. What do you need to do to make Samba reread the configuration file?
5. Test the result, first from the prohibited host specified in Step 3, and then from a second host on the local network.
6. Bonus lab: take the steps required to reinstall Samba and the associated original version of the smb.conf configuration file.

Lab 4

In this lab, you'll customize the default **[homes]** share for specific user-based security requirements. You'll need one common user on both the local Samba server and a remote Samba client.

1. Open the main Samba configuration file.
2. Navigate to the predefined **[homes]** share.
3. Ensure that the **[homes]** share is available only to hosts on the local example.com network. Alternatively, you can allow access to all systems on a local network, except for one IP address.
4. Ensure that the share is writable to one authenticated user.

5. Set up that one user in the Samba password database.
6. Test the result from a remote system. If possible, test the result from systems both within the example.com network and outside that network. Alternatively, make the tests from systems that are supposed to be allowed and denied as configured in Step 3.

Lab 5

In this lab, you'll go a step further and create a public share accessible to all users.

1. Create a new share called **[public]**.
2. Change the path to the public share to /home/public.
3. Configure the public share so that anyone in the local example.com domain can access the share.
4. Create the /home/public directory as required. Change the permissions to this directory to 1777.
5. What is the advantage of 1777 permissions?
6. Commit your changes.
7. Test the result from a remote system. What happens if you write a file to that shared directory?

Lab 6

In this lab, you'll go even further and create a shared directory, with access limited to a group of two users. The basic steps are the same as Lab 5; however, you'll need to create a directory with SGID permissions, along with full permissions to the group owner of that directory. The basic steps to create that shared directory are the same as that created in Chapter 8.

Then, create a user account with minimal permissions, which will be used for authentication with the **mount.cifs** command. Test the result from a remote system and mount the Samba share persistently in /etc/fstab with the **multiuser** option. As a normal user, run the **cifscreds** command to store the access credentials in the user's keyring before accessing the share.

Lab 7

It is important for a server that any changes made are persistent. This means that changes should be active when you reboot Linux. Perform an orderly reboot of the local server now and verify that Samba starts when you boot Linux.

1. How did you make your changes persistent?
2. What command did you use to perform an orderly shutdown?
3. What changes to SELinux settings should you verify?