# Chapter 9 Lab Questions

During the RHCSA exam, 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 9. Most of the labs for this chapter are straightforward and require a very few commands or changes to one or two configuration files.

## Lab 1

Install the tuned RPM package and ensure that is started and enabled at boot.

Find the current active tuned profile and switch the system to the balanced profile.

Reboot the system and confirm that the balanced profile is the active one.

Finally, restore the default profile.

## Lab 2

As the root user, create cron jobs that change the login message for users at the text console. To do so, you’ll want to change the content of /etc/motd. Make sure that people who log in at different times get appropriate messages:

If users log in between 7 a.m. and 1 p.m., create the login message “Coffee time!”

If users log in between 1 p.m. and 6 p.m., create the login message “Want some ice cream?”

If users log in between 6 p.m. and 7 a.m., create the login message “Shouldn’t you be doing something else?”

## Lab 3

In this lab, you’ll set up an at job as the root administrative user, to save a list of currently installed RPMs in the /root/rpms.txt file. That job will be run once, 24 hours from now. If you want to verify your work, set up a second at job with the same commands to start five minutes from now.

## Lab 4

In this lab, you’ll set up a cron job to back up the /etc directory every Saturday at 2:05 a.m. You should ensure that SELinux contexts are preserved. You are not allowed to edit the root crontab. The backup should be saved in a gzipped-tar archive format in the /tmp directory, using the filename etc-backup-MMDD.tar.gz, where MMDD is the current date in numeric format. Extract one of the generated backup files, to confirm that SELinux contexts are preserved.

## Lab 5

In this lab, you'll create a script that can be used to backup any given directory to a specified destination directory. The script should:

1. Accept two arguments: the first argument represents the source directory to be backed up, while the second argument represents the destination directory where the backup will be stored. If the specified directory doesn’t exist, the script should create it.
2. Name the backup file in the format backup-MMDDHHSS.tar, where MMDDHHSS is the current month, day, hour, and second.
3. Check the number of arguments passed to the script. If they are not equal to two, the script should display a usage message and exit.
4. Confirm that the first argument passed to the script represents an existing directory. If not, the script should display an error message and exit.
5. Confirm that the second argument is a directory. If it doesn't exist, create it.
6. For this lab, do not consider the scenario where the second argument is a file but not a directory.

## Lab 6

In this lab, you’ll find the value of several different log files. In preparation, use the wrong password to log in to a regular account. Then take the following steps:

1. Navigate to /var/log as the root user. All of the files listed in this lab are in that /var/log directory.
2. Explore the contents of the anaconda.\* log files.
3. Run the **utmpdump btmp** command. Do you see the login attempt? Can you tell if it succeeded?
4. Review the contents of the cron log file. Scroll through it. If your computer has been on for a while, most of what you see will be based on the **run-parts /etc/cron.hourly** command. Alternatively, if you reboot on occasion, you’ll see messages associated with the anacron service.
5. Run the **dmesg | less** command to print the content of the kernel ring buffer. Compare the beginning of it with the start of the anaconda.syslog file. Which one includes the currently booted kernel?
6. Navigate toward the end of the output of the **dmesg | less** command. Can you identify the amount of swap space? Can you identify one or more partitions with the default XFS filesystem?
7. Review the maillog log file. If that file is short, there may be an older maillog-\* file; if so, review that as well. Do you see any logs associated with mail messages?
8. Review the secure log file. Navigate to the bottom of the file. Do you see a message associated with failed logins?