01 Performing Basic Linux Tasks

Entering Shell Commands

> Scenario

```
You are a systems administrator at Develetech. As a result of your earlier
discussion with the IT team at Develetech, your CTO is becoming more and more
convinced of the viability of switching the company's server infrastructure to
Linux. The CTO wants you to become more familiar with using Linux, and he suggests
doing so by booting up a test machine and trying it out. So, you'll start by
entering some basic commands at the Bash shell to get a feel for the Linux
environment.
```

> Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
  2.3 Given a scenario, create, modify, and redirect files.
  3.1 Given a scenario, apply or acquire the appropriate user and/or group
permissions and ownership.
```

1. Whenever the instruction states "*enter command*", you are required to type the command and press Enter. Note that Linux commands, command-line options, and file names are case-sensitive.
    - Some of the commands in the course activity steps spill over onto the next line. Unless specified otherwise, all commands should be entered on the same line in the CLI.
2. Log in and use basic navigation commands
    - At the localhost login prompt, enter `student01`
    - At the Password prompt, enter `Pa22w0rd`
        - Be careful when you type in passwords, as the CLI does not show them on screen.
    - Verify that you are presented with a `[student01@localhost ~]$` prompt, indicating that you have successfully logged in.
    - At the prompt, enter `echo 'Hello, World!'`
        - Recall that you cannot use the automatic Type Text feature with Linux virtual machines and that all commands and input in Linux are case-sensitive. Linux commands will be displayed by using the monospace font: `hostname`
    - Verify that the console printed the string `Hello, World!` back to you.

- Enter `pwd` to retrieve information about your current working directory.
- Your current working directory is `/home/student01`
- Enter `ls` (lower case L+s) and note the contents of your current working directory.
- At the moment, there doesn't seem to be anything in your home directory.
- Enter `ls -a` to display hidden items.
- Now, you can see that there are files and folders in this directory, but they are hidden from a standard directory listing.
- Enter `ls -al` and note that you are given more information about each item in the directory.
- The name of the file or folder is on the right. The last modified date and time is to the left of the name, and to the left of that is the size of the file or folder (in bytes). Most of the other fields relate to permissions and ownership.
- Enter `cd /etc` to change your current working directory.
- Verify that the prompt has changed to `[student01@localhost etc]$`
- Enter `pwd` to further verify that your current working directory is now `/etc`
- Enter `cd /var/log` to move to the directory where system log files are stored.
- Enter `ls -al` to see all of the files and folders that exist in this directory.
- Enter `cd /home/student01` to move back to your home directory.
- Enter `touch myfile` to create an empty file in your home directory.
- Enter `ls` and verify that myfile is listed in the directory.
- Enter `cat /etc/hostname` to view the hostname file by using the `cat` command.
- Verify that the contents of the `/etc/hostname` file are printed at the CLI.
- Enter `cat /var/log/dmesg` to display information about the boot process.
- Verify that this log file is so long that much of its contents scroll past the screen.
- The cat command has no navigational options, so you'll need to use a more advanced command to view all of the log file.
- Enter `less /var/log/dmesg` to view the file by using the `less` command.
- Instead of scrolling, the `less` command printed only the beginning contents of the file that fit on the screen. Your prompt has also changed to the name of the file, highlighted.
- Scroll down by using `Enter` or the `Down Arrow` keys. Scroll down a few lines.
- Press `y` or `Up Arrow` to scroll up one line.

- Scroll up a few more lines.
- Press `Spacebar` or `Page Down` to scroll down an entire screen.
- Press `b` or `Page Up` to scroll up an entire screen.
- Press `q` to quit viewing the file and return to your regular prompt.

3. dit a text file by using Vim

- Enter `vim myfile` to open the file you created earlier in the Vim text editor.
- Press `i` to switch to Insert mode.
- Type `Hello, this is Student01`.
- Press `Esc` to switch back to Command mode.
- Enter `:wq` to write (save) the file and quit.
- Enter `cat myfile` and verify that the contents of the file are printed to the CLI.

4. Create and edit a text file with GNU nano.

- Enter `nano myfile2` to create and begin editing a new file.
- Type `Hello, this is Student01.`
- Press `Ctrl+O`, then press `Enter` to save the file.
- Press `Ctrl+X` to quit.
- Enter `cat myfile2` and verify that the contents of the file are printed to the CLI.
- Enter `clear` to clear the screen.

5. Assume superuser privileges.

- Enter `cat /var/log/boot.log`
- Verify that you are given a Permission denied error.
- As a regular user, you do not have permission to read this log file. You need to elevate your privileges to do so.
- Enter `su - root` to switch user to the root (administrator) account.
- There is a space on either side of the dash in the `su - root` command.
- At the Password prompt, enter `Pa22w0rd`
  - The passwords for your student account and the root account are the same for lab convenience. In a production environment, the root password should be unique and not based on a common dictionary word.
- Verify that your prompt has changed to `[root@localhost ~]#`
- You are now logged in as the root user, the user with the highest level of privileges (superuser).
- Enter `cat /var/log/boot.log` and verify that you can now read the file.
- Enter `exit` to log out as root and switch back to your regular student account.

6. Use tab completion to make typing commands more efficient.

- Enter `touch thisisalongfilename.txt`
- Type `ls -l th` and then press `Tab`.
- Verify that the rest of the file name is filled at the command-line.
- Press `Enter` to execute the command.

7. View the command history.

- Type `his` and press `Tab`.
- Verify that the history command is populated at the command-line.
- Tab completion works on file, directory, and even command names.
- Press `Enter` to execute the command.
- Verify that a list of the commands you recently entered is printed on the screen.

8. Restart the computer.

- Enter `reboot`
- Verify that the computer restarts, and then prompts you to log in.
- Log in as `student01` with `Pa22w0rd` as the password.

Accessing Help in Linux

> Scenario

```
In order to be useful, Linux must have tools with certain capabilities that will
be useful to the business. One of these capabilities is searching the contents of
text files. This will come in handy for administrators who need to efficiently
analyze text files like system logs, automated scripts, etc., for specific
patterns. You'll need to find one or more Linux tools that can accomplish this and
learn how to use them. So, you'll consult various help resources to get acquainted
with the appropriate tool(s).
```

> Objectives Completing this activity will help you to use content examples from the following syllabus objectives: 2.3 Given a scenario, create, modify, and redirect files

1. Look for a command that could help you search the contents of a text file.

- If necessary, log in as `student01` with a password of `Pa22w0rd`
- Enter `apropos search`
  - If you get nothing appropriate as the result of the apropos command, enter `su - root` and enter `Pa22w0rd` when prompted. Then, enter `mandb` to update the database. After the command finishes running, enter `exit` to return to your `student01` account and enter `apropos` search again.
- Verify that multiple commands are listed in the output, each of which includes the term search in its name or brief description.
- You could try to pick out the appropriate command from these results, but changing your search might narrow them down.
- Enter `clear` to clear the screen.
- Enter `apropos pattern`
- Verify that you receive fewer results.
- Looking at these results, which command(s) do you think would best fulfill the capabilities that you're looking for? Click here for the answer
  - Answers may vary, but one of the `grep` variants is likely the most appropriate command. The `awk` command and its variants could be helpful, but appear to be more advanced.

2. Read the manual page for a command that could be what you're looking for

- Enter `man grep`
- Verify that you see the manual page for the `grep` command.
- Read the `SYNOPSIS` section to understand how to use the command.
- Read the `DESCRIPTION` section to understand what the command does.
- Navigate up and down the man page using the same keys as the `less` command.
- Enter `/case` to search the man page for the term "`case`".
- Press `n` to navigate to the next instance of the search term.
- When you're at the end of the man page, press `Shift+N` to navigate to the previous instance of the search term.
- Read the description for the command option that has to do with case.
- Given what you've read in the `man` page for `grep` so far, answer what you think the following command does: `grep -i hello myfile`
- Click here for the answer

3. Search for more information about the `grep` command.

   - Press `q` to quit the man page.
   - Enter `cd /usr/share/doc`
   - Enter `ls`
   - Verify that there are many subdirectories in this directory, each of which corresponds to a software package.
   - Type `cd grep` and press `Tab`.
     - Make sure not to add a space after `grep` before you press `Tab`.
   - Verify that the path to the specific version of `grep` is completed, then press `Enter`.
   - Enter `ls`
   - Enter `less NEWS` and then briefly skim the change notes for the `grep` command.
   - Press `q` to quit.
   - How confident are you that this command fulfills what you're looking for? Click here for the answer

     ```
     Answers may vary, but the grep command does generally meet your
     requirements. However, this doesn't mean it's the only command, or the
     best command, for the job.
     ```

   - You still want to learn more about other commands that your team could use to search the contents of a text file. Aside from the help options built into Linux, what other sources can you consult in your research? Click here for the answer

     ```
     ```

```
Answers may vary, but there is a wide variety of useful sources on the
Internet that could help you find what you're looking for. You could
pose specific answers to Q&A sites like Stack Exchange; ask discussion
questions on newsgroups, mailing lists, and forums dedicated to Linux
support; consult supplementary and/or advanced documentation through a
resource like the Linux Documentation Project; or consult distro-
specific documentation on the relevant distro's website.
```

Managing Users And Groups

> Scenario

While investigating Linux on behalf of Develetech, you have found multiple warnings about the danger of using the root user administrative account. You are already familiar with the principle of least privilege, which states that users should be granted only the level of access they need and no more. You also know that this applies to administrators as well as to end users. The Develetech security policy states that administrative privileges must be carefully controlled. You need to report on how this requirement can be satisfied.

> Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   3.1 Given a scenario, apply or acquire the appropriate user and/or group
permissions and ownership.
```

---

1. Use the `su` and `sudo` commands
    - Log in as `student01` with the password `Pa22w0rd`
    - Enter `id` to verify that you are currently signed in as `student01`.
        - Recall that you cannot use the automatic Type Text feature with Linux virtual machines and that all commands and input in Linux are case-sensitive. Linux commands will be displayed by using the monospace font: hostname
    - Enter `su root` to elevate your credentials to those of root.
    - Enter the `Pa22w0rd` password.
    - Enter `id` to verify the root user login.s
    - Enter `pwd` to confirm the present working directory. **Note** that while your credentials are those of the root user, your location and context are those of the student01 user. You are essentially logged in as root in the student01 user environment.
    - Enter `exit` to return to the `student01` user login.
    - Enter the `su - root` command to elevate your credentials and context to those of root.
        - There is a space on each side of the hyphen.
    - Enter the `Pa22w0rd` password.
    - Enter `pwd` to confirm the present working directory.
        - Note that both your credentials and your context are those of the `root` user. You are now logged in as `root` in the `root user environment`. If you use the `su` command without an argument, the system will default to the root user. Example: `su - assumes su - root`
2. Delegate administrative privileges to the student account.
    - Enter `visudo` to start editing the `sudoers` file. In the previous section you elevated your credentials to root, which permits you to do anything on the system. Any mistakes could be catastrophic. It is a better security practice to delegate specific tasks by using the sudo command.

- Press `Page Down` several times to move the cursor to the bottom of the file. Alternatively, you can press `Shift+G` to move directly to the last line of the file.
- Press End to move to the end of the last line.
- Press o to enter Insert mode and start a new blank line below the current line.
- Add the following text on a new line:

```
student01 ALL=(ALL) NOPASSWD:ALL
```

This grants the student account the ability to execute all commands without you having to switch to the root user every time. It also prevents you from having to input your password. This is for lab convenience and is not suggested on a production environment.

- Press `Esc` to exit insert mode.
- Enter `:wq` to save and close the file.
- Enter `exit` to return to your `student01` account.
- Enter `id` to verify that you are signed in to your `student01` account.
- Enter `exit` again to log out of the system.
- Log back in as `student01` using `Pa22w0rd` as the password.
- Enter `sudo /sbin/shutdown -r 15` to test your ability to shutdown the machine.
  - This command tells the system to reboot after a fifteen minute delay. It requires **administrative privileges**. You are executing the command with sudo in order to temporarily leverage those privileges.
- If you ever forget to add `sudo` to a privileged command, enter `sudo !!` to re-issue the most recent command with `superuser` privileges.
  - Press [Ctrl+C], and then enter the `sudo shutdown -c` command to interrupt the reboot.

Creating User Accounts

Scenario

```
Managing user and group accounts in Linux will be a key administrative
responsibility at Develetech. Now that you have become comfortable with some basic
Linux commands, you need to become proficient at managing users. You'll start by
creating some user accounts and viewing their defaults.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
• 2.2 Given a scenario, manage users and groups
```

---

1. View the current default settings for new users.

- Enter `sudo useradd -D` to view the default settings for newly created users.
- Enter `less /etc/login.defs` to view the default settings for newly created users.
- Press `q` to quit.
- Enter `ls -a /etc/skel` to view files that will be copied to the home directories of newly created user accounts.

2. Create a user

- Enter `sudo useradd manderson` to create a new user account for Michael Anderson named `manderson`.
- Enter `cat /etc/passwd` to view the new user account in the `/etc/passwd` file.

3. Newly created user accounts are appended to the bottom of this file.

- Enter `sudo useradd -c "Chris Mason" cmason` to create a new user account for Chris Mason named `cmason`. This command creates the `cmason` account and populates the comments field of the account with the user's full name.
- Enter `cat /etc/passwd` to verify that the newly created user account at the bottom of the screen also includes a "comment" consisting of the user's full name.
- Create new user accounts for `Andrew Riley` and `Rachel Alexander` named `ariley` and `ralexander`, respectively by using the following commands:

```
sudo useradd ariley
sudo useradd ralexander
```

- Create a *new temporary user account* for `Rose Stanley` named rstanley whose contract will end on December 31, 2025 by using the following command:

```
sudo useradd -e 2025/12/31 rstanley
```

- Enter `cat /etc/passwd` and note the newly created account.

Modifying User Accounts

> Scenario

```
Now that you have configured a few standard user accounts, you want to ensure the
accounts exist. You also need to set password requirements. In addition, you will
investigate whether password expirations can be configured and whether user
accounts can be locked if users take a leave of absence.
```

> Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: • 2.2 Given a scenario, manage users and groups

1. Modify user accounts

    - Enter `cat /etc/passwd` to display the contents of the `/etc/passwd` file.
    - Verify that, for each user account, the password field shows an `x` character.
        - The x character is a placeholder that indicates that the password hash is actually stored elsewhere.
    - Enter `sudo cat /etc/shadow` to display the contents of the `/etc/shadow` file.
    - Verify that you can see various information about each user account, including their password hash value and any expiration information.

2. The `!!` symbols indicate that the account has a blank password and therefore users are not allowed to log in as that account.

    - Enter `sudo passwd manderson` to configure a password for the `manderson` account.
    - When prompted for the password, enter `Pa22w0rd`
        - You can ignore the warning about this password failing a dictionary check. In a production environment, you'd choose a much stronger password.
    - When prompted to retype the password, enter `Pa22w0rd` again.
        - Recall that Linux will not display any characters on the screen representing the new password.
    - Repeat these steps to add the password for the `cmason`, `rstanley`, `ariley`, and `ralexander` accounts.
    - Enter `sudo cat /etc/shadow` and note that the password hash fields are now populated for these users.

3. Attach a real name to each user account.

    - Enter `sudo usermod -c "Rose Stanley" rstanley` to modify the comment field for the existing `rstanley` account.
    - Repeat the previous step for each of the following user accounts:

```
manderson – Michael Anderson
ariley – Andrew Riley
ralexander – Rachel Alexander
```

    - Enter `cat /etc/passwd` to display the modifications.
    - Enter `sudo chage -l manderson` to display the *manderson account password expiration information*.
    - Enter `sudo chage -E 2026/12/31 manderson` to set the account expiration for the user to 12/31/2026.
    - Enter `sudo chage -l manderson` to view the updated expiration information.
    - Enter `sudo passwd -l cmason` to lock the `cmason` account.
    - Enter `sudo passwd -u cmason` to unlock the `cmason` account. Note the warning message.
    - Enter `sudo usermod -L cmason` to lock the `cmason` account.
    - Enter `sudo usermod -U cmason` to unlock the `cmason` account.

Deleting a User Account

> Scenario

```
You recognize that part of the user account lifecycle is the deletion of accounts
that are no longer needed on the system. You will use the userdel command to
delete a test account.
```

> Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
• 2.2 Given a scenario, manage users and groups
```

- Enter `cat /etc/passwd` and confirm the `ralexander` account exists.
- Enter `sudo userdel ralexander` to delete the `ralexander` account.
- Enter `cat /etc/passwd` and confirm the `ralexander` account has been deleted.
- Enter `ls /home` and observe that the `ralexander` home directory still exists.

NOTE: By default, the `userdel` command deletes the user account but not the user's home directory. If you include the `-r` option, the user's home directory will be deleted with the user account.

Creating, Modifying, and Deleting Groups

> Scenario

```
You will need to associate several user accounts together into groups to make IT
management at Develetech easier. You will create several groups that correspond to
different departments. At some point, you'll need to rename the Graphics group to
fit the naming scheme of the other groups. In addition, you will add users to the
groups. Part of the user/group management lifecycle dictates that you'll
occasionally need to delete groups. So, you'll finish by deleting a group, but not
the users that are part of that group.
```

> Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
• 2.2 Given a scenario, manage users and groups
```

---

1. Create a new group called Graphics.

- Enter `cat /etc/group` to view the current groups on the system.
- Enter `sudo groupadd Graphics` to create a new group called Graphics.
- Repeat this step to create three additional groups with the following names:
  - `SalesDept`
  - `MarketingDept`
  - `FinanceDept`
- Enter `cat /etc/group` and note the presence of the four new groups.
- Observe the current Graphics group name, and then enter `sudo groupmod -n GraphicsDept Graphics` to rename the Graphics group to GraphicsDept
- Enter `cat /etc/group` and view the new group name.
- Enter `sudo usermod -aG GraphicsDept rstanley` to add the rstanley account to the GraphicsDept group.
- Repeat this step to add the following users to the following groups:
  - `FinanceDept – manderson`
  - `SalesDept – cmason`
  - `MarketingDept – ariley`
- Enter `cat /etc/group` and confirm that each user is a member of their assigned group.
- Confirm that the `SalesDept` group exists.
- Enter `sudo groupdel SalesDept` to delete the `SalesDept` group.
- Enter `cat /etc/group` to view the existing groups.
- Confirm that the `SalesDept` group has been deleted.
- Enter `cat /etc/passwd` to view the existing users.
- Confirm that deleting the `SalesDept` group did not delete the `cmason` user account, even though it was a member of that group.

Querying Users and Groups

> Scenario

```
There are several ways a user can gather information about their own account and
group memberships. In addition, there are multiple ways of identifying what users
might currently be logged on the system. You will explore these methods to ensure
you can answer questions the users you support might have. The Develetech security
policy requires that a log file of user logins be kept in case of an audit or
security incident.
```

> Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: • 2.2 Given a scenario, manage users and groups

---

1. Display group information

- Enter `su - root` and the password `Pa22w0rd` to switch to the `root user`.
- Enter `whoami` to display your login name.
- Enter `id` to display your login credentials and group membership.

- Verify that the command prompt shows the `root` name and a `#` character.

2. The `#` character in the prompt also indicates that you are signed in as the `root` user. For standard users, the prompt will show a `$` character.

   - Enter `exit` to leave the `root` login and return to your `student01` account.
   - Enter `whoami` to display your login name and to verify your student account credentials.
   - Enter `id` to display your login credentials and group membership.

3. Verify that the command prompt shows the `student01` name and a `$` icon.

   - Enter who to see what users are currently logged in to the system.
   - Enter `w` to see what users are currently logged in.
   - Compare `who` and `w` for details, and then observe the idle time information.
   - Enter `last` to display a record of recent logins to the system.

Configuring Account Profiles

> Scenario

```
You're concerned that a change to Linux systems may be difficult for users. You
need to identify what files can be used to make the user command-line environments
customized and consistent. In addition, you need to place a copy of the Develetech
policies in each new user's home directory for reference.
```

> Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
• 2.2 Given a scenario, manage users and groups
```

---

1. Display the contents of the `.bashrc` file

   - Enter `cat .bashrc` to view the configuration file for the student account.
     - Notice that there are no preconfigured alias settings for standard users in CentOS 7.
   - Enter `sudo cat /root/.bashrc` to view the configuration file for the root user.
     - Notice that the root user's profile includes alias settings for the copy, move, and delete commands, setting them for interactive mode. These are default alias settings for the root user in CentOS 7.
   - Enter `cat .bash_profile` to view the contents of the configuration file.
     - The `.bash_profile` file is called when the user first logs in. Observe that the file contains the `PATH` variable setting, which defines where Bash will search for command executables.

2. Manage the `/etc/skel` directory

   1. Enter `ls -a /etc/skel` to view the files currently in this directory.

2. Enter `sudo touch /etc/skel/policies.txt` to create a file in the directory.
3. Enter `sudo useradd jrobinson` to create a new user account for Jerry Robinson.
4. Enter `sudo ls -a /home/jrobinson` and note the presence of the `policies.txt` file. This file was copied as part of the `useradd` tool.

3. Configure the `jrobinson` user account

   - Enter `sudo usermod -aG GraphicsDept jrobinson` to add `jrobinson` to the *GraphicsDept group*.
   - Enter `sudo usermod -c "Jerry Robinson" jrobinson` to provide a full name in the comments field.
   - Enter `sudo passwd jrobinson` to set a password for the account.
   - Enter `Pa22w0rd` as the password.

Managing Files and Directories

Creating Text Files

Scenario

```
As one of the Linux server administrators, you've been asked to start a list of
software that is installed or should be installed on the system. So, you'll create
a text file and begin entering the names of software packages into it. You'll then
save your work and pick up with the file later.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   2.3 Given a scenario, create, modify, and redirect files
```

1. Create the software list file by using the Vim text editor
   - Log in as `student01` with `Pa22w0rd` as the password.
   - Verify you are in your `home` directory.
   - Enter `vim software_list.txt` to start editing a new file in Vim.
   - Press `i` to switch to Insert mode.
   - Recall that Vim has three modes. Each mode may be thought of as a keyboard mapping. When you are in Insert mode, the keyboard inserts text into the file. When you are in Command or Execute mode, the keyboard issues commands to the Vim program.
   - Verify that the text "`INSERT`" is displayed at the bottom-left of the screen.
   - On the first line, enter `Apache HTTP Server`
   - Enter `MySQL` on the second line.
   - Enter `Eclipse` on the third line.
   - Type `OpenVAS` as the fourth and final entry.
   - Your Vim file should look like the image below:

```
Apache HTTP Server
MySQL
Eclipse
OpenVAS
~
~
~
~
~
~
-- INSERT --                    4,8
```

- Press `Esc` to return to Command mode.
- Remember that `Esc` returns you to Command mode. The lower case `i` moves you from Command mode to Insert mode, though there are other keys that have a similar function. The colon : moves you from Command mode to Execute mode, which gives you a command prompt within Vim.
- Enter `:wq` to write (save) your changes to the file and quit Vim.
- Enter `cat software_list.txt` to view the file.

Editing Text Files

Scenario2

```
A colleague has taken your initial software list file and started filling it out.
After he's done, you look it over to see if there are any mistakes that need
correcting. You'll edit this file in both Vim and GNU nano to become more familiar
with both text editors.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   2.3 Given a scenario, create, modify, and redirect files
```

1. Copy the latest version of the software list
   - Enter `cp -a /opt/linuxplus/managing_files_and_directories/software_list.txt ~`
   - Remember, you can use `tab completion` to speed up the process.
   - Enter `ls` and verify that `software_list.txt` is listed.

2. Open the file in `Vim` and correct a spelling error
    - Enter `vim software_list.txt` to open the file. Remember that Vim opens in Command mode.
    - Use the arrow keys to move the cursor down to the first instance of the text "`Friefox`".
    - Position the cursor under the "`i`" in "`Friefox`".
    - Press `x` to cut the letter "`i`".
    - Move the cursor under the letter "`F`" and press `p` to paste the cut letter.
    - Verify that the line now correctly says "`Firefox`".
3. Use the search functionality built into Vim to find and correct the other instance of the spelling error
    - Enter "`/Frie`" to search for the next occurrence of the misspelled name.
    - You use the `/` to create a command prompt at the bottom of Vim and then you enter the text you wish to search for.
    - Correct the name so that it says "`Firefox`".
4. Fix the casing of one of the software names
    - Press `k` to go up line-by-line until you reach the line that says `"openVAS"` (note the lowercase "o").
    - Press `^ (Shift+6)` to go to the beginning of the line.
    - Press `x` to delete the first letter.
    - Press `i` to enter Insert mode, then type an uppercase O
    - Press `Esc` to exit Insert mode and return to Command mode.
5. Delete a duplicate line and save the file
    - Press `j` to go down line-by-line until you reach the second line that mentions `Apache`.
    - Press `d` twice to delete the entire line.
    - Enter `:wq` to write your changes and quit the file.
6. Open the file in `GNU nano` and make a correction
    - Enter `nano software_list.txt` to open the file in the nano text editor.
    - The nano text editor is common on many Linux distros. You should know the basics of both Vim and nano.
    - Use the arrow keys to move to the `Y` under the "`Configured?`" column for "`Eclipse`".
    - Press `Delete`.
    - Type `N`
7. Remove a duplicate line
    - Navigate down to the **second** instance of "`LibreOffice`".
    - Press `Ctrl+K` to cut the duplicate line.
    - Note that some of the most common key commands for nano are displayed at the bottom of the window. There are many other key commands as well.
8. Add another entry to the file
    - Navigate to the beginning of a new line at the bottom of the file.
    - Type `Apache-Tomcat`
    - Press Tab until the cursor is under the "Version" column.
    - You can also use the spacebar for more precise alignment.
    - Type `9.0.12`
    - Place the cursor under the "`Installed?`" column and type `N`
    - Type `N` under the "`Configured?`" column.
    - Press `Ctrl+O` "write out" or save you changes to the file.
    - Press `Enter` to save the file.
    - Press `Ctrl+X` to exit GNU nano.

- Enter `cat software_list.txt` to display the file.

Searching for Files

Scenario3

```
One of your duties as a Linux administrator is to ensure your system logs are
functioning as expected. These logs are crucial to diagnosing issues and
identifying other unwanted behavior. So, to start, you'll search for where the log
files are stored on your system. Then, you'll begin to search for logs that meet
specific size requirements and have been recently updated. That way you'll be able
to confirm which logs are continuously recording a significant amount of
information, as expected.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   2.3 Given a scenario, create, modify, and redirect files
   3.4 Given a scenario, implement logging services
```

1. Search for the location of system log files.

    - Enter `sudo find / -type d -name 'log'` to search the root of the filesystem `/` for a directory `d` with a name that includes the string `log`.
    - Verify that there are several locations on the root volume that contain the word `log`.
    - Enter `sudo find / -type f -name 'messages'` to search the root of the filesystem `/` for a file `f` with a name that includes the string `messages`.
    - Verify that the location of the messages `log` is identified as `/var/log/messages`
    - Enter `sudo find /var/log -type f -size +100k` to search for log files that are greater than 100 KB in size.
    - Pick one of the files in the results and enter `ls -lh /var/log/[file name]` to verify that it is indeed greater than 100 KB in size.
    - Enter `sudo find /var/log -type f -mmin -30` to search for log files that have been updated within the last 30 minutes.
    - Verify that one of the files in the results has a timestamp within the last 30 minutes.
    - You can use `ls -l` on the file to display details about the file, including when it was last modified.
    - Enter `sudo find /var/log -type f -size 0 -or -size +100k -mmin -30` to search for log files that are either empty or above 100 KB, and have been updated in the last 30 minutes.

- Verify that these conditions are accurate for at least one of the files.
- What are some advantages of using the find command over using the locate command? Click here for the answer.

```
The locate command requires that a database be updated in order to
perform accurate searches, whereas find does not. Also, locate cannot
filter its search by specific directories, whereas find can. However,
locate may be able to perform searches more quickly in certain cases.
```

Reading Files

Scenario4 Another one of your duties is, naturally, to review the system's log files. But before you dive into log analysis, you need to determine the best way to display text files for reading. So, you'll use commands like cat and less to see where each one can come in handy.

Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: 2.3 Given a scenario, create, modify, and redirect files

1. Reading logs
   - Enter `sudo cat /var/log/messages` to open the messages log for reading.
   - Notice that the file's contents scroll past the screen many times, indicating that the file is too large to read from a single screen.
   - Enter `sudo less /var/log/messages` to display the file by using the less command.
   - Verify that only the first page of the file printed to the screen, and at the bottom of the screen, the name of the file is highlighted.
   - The less utility breaks a long file down into pages that fit on the screen. You can then scroll through the pages.
   - Press the `Down Arrow` to scroll down a single line.
   - Press the `Up Arrow` to scroll back up a single line.
   - Press `Space bar` to scroll down an entire page.
   - Press `Page Up` to scroll up an entire page.
2. Search for a specific string in the log.
   - Enter `/SELinux` to search for the string SELinux.
   - Note that this is the same search syntax as you used in the `Vim text editor`.
   - Verify that the file jumps to the first instance of this text string, and that it is highlighted on the top line.
   - Press `n` to view the next instance of this text string in the file.
   - Press `N` (note the capitalization) to navigate to the previous instance of the search term in the file.
   - Press `q` to quit reading the file.
   - Remember, you can enter `clear` to clear the screen as needed.
3. Display only the first and last lines of the log
   - Enter `sudo head /var/log/messages` to display the first several lines of the file.

- Verify that the *first 10 lines* of the messages log were printed to the screen.
- Enter `sudo tail /var/log/messages` to display the last several lines of the file.
- Verify that the *last 10 lines* of the messages log were printed to the screen.
- Why might displaying only the first or last few lines be preferable to reading the entire file? Click here for the answer.

```
Answers may vary, as it depends on the purpose and format of the text
file. For logs, reading the last 10 lines is a much quicker way to see
the latest events on a system than using less would be. Printing the
first 10 lines might be useful in situations where entries are repeated
or otherwise superfluous, and you only need to see a few examples to
grasp the idea.
```

Manipulating Files and Directories

Scenario5

```
You've been asked to move some corporate policy documents from the HR lead's
workstation to a Linux server. The policies should be more centrally available and
not dependent on one particular person's system. The HR lead admits that she
didn't do a great job organizing the policy documents, as several older versions
of acceptable use policies (AUPs) are mixed in with more current, active versions,
and the old policies were written before she implemented a consistent naming
convention. All of the documents are in a single directory named aups.
First, you'll need to copy the documents to your home directory as a temporary
staging area. You'll then organize these policy documents by retaining only the
most recent ones and deleting older ones that no longer apply. You've also been
told that more types of policies will need to be located on the server, other than
AUPs. So, you'll effectively rename the aups folder to the more general policies
and create some placeholder files. Later, when you receive more policies to add,
you'll be able to deploy the directory where other authorized users can reach it.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   2.3 Given a scenario, create, modify, and redirect files
```

1. Manipulate
   - Enter `cp -r /opt/linuxplus/managing_files_and_directories/aups ~` to copy the aups directory to your home directory.

- This copies the `aups` directory to your home directory, leaving its original location intact.
- Enter `cd aups` to change directories.
- Enter `ls -l` and verify there are five files, three of which are marked as "OLD" and have inconsistent file names.

```
[student01@localhost aups]$ ls -l
total 20
-rwxr-xr-x. 1 student01 student01 1472 Dec 14 14:15 aup_v1.txt
-rwxr-xr-x. 1 student01 student01 1878 Dec 14 14:15 aup_v2.txt
-rwxr-xr-x. 1 student01 student01  794 Dec 14 14:15 OLD acceptable_use2.txt
-rwxr-xr-x. 1 student01 student01  353 Dec 14 14:15 OLD acceptableuse.txt
-rwxr-xr-x. 1 student01 student01 1015 Dec 14 14:15 OLD acct use3.txt
```

2. Create a new directory and move the most recent policy files into it

- Enter `mkdir ../policies` to create a new directory.
- Enter `mv aup_v1.txt ../policies` to move the file.
- Enter `mv aup_v2.txt ../policies` to move the file.
- Enter `ls -l` and verify that these two files are no longer in this directory.
- Enter `cd ../policies` to change to the policies directory.
- Enter `ls -l` and verify that the two recent files are now in this directory.

3. Create placeholder files for future policies

- Enter `touch user_sec_policy.txt` to create a new empty file named `user_sec_policy.txt`
- Enter `ls -l` and verify that a blank file with this name was created.
- Use `touch` to create three more blank files in `~/policies` with the following names:

```
- server_sec_policy.txt
- email_policy.txt
- clean_desk_policy.txt
```

- Enter `ls -l` and verify that the files exist.

4. Delete the aups directory and its contents as it is no longer needed

- Enter `rmdir ../aups`
- Verify that you cannot remove this object because it is a directory with contents.
- You need to specify the `-R (recursive)` option with `rm` in order to delete non-empty directories.
- Enter `rm -R ../aups` to delete the directory and its contents.
- Enter `ls ..` and verify that the `aups` directory is gone, as are the old policy files.

Processing Text Files

Scenario6

```
Now that the software list and policy documents are all set and in the right
locations, you can begin to analyze them more closely. In particular, you want to
```

```
sort the software list so you can more quickly identify what software packages
still need to be installed and/or configured. Likewise, you want to ensure that
you know exactly what was changed from the first version of the AUP to the second
version, so you don't have to read the entire thing from the beginning.
You also want to switch gears to your log analysis duties. You want to identify
instances where users enter an incorrect password and fail to log in. This could
point to users that are trying to access resources they are not authorized for.
However, the authentication log can be very large, so you'll need to process it in
order to extract only the relevant information.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    2.3 Given a scenario, create, modify, and redirect files
```

1. Sort the software list file by name, then by which packages need to be installed and/or configured.
    - Enter `cd ~` to return to your home directory.
    - Enter `cat software_list.txt` to review the column structure of this file.
    - Enter `sort -k1 software_list.txt`
    - Verify that the list was sorted by the first column, which is the name of each software package. However, the sort operation was not perfect, as the column headers were included. There are several ways to stop this from happening, one of which you'll perform in a later topic.
    - Enter `sort -k3 software_list.txt` to sort by the "Installed?" column.
    - Sort by the "`Configured?`" column.
2. Retrieve the word count of the AUP files.
    - Enter `cd policies` to change directories.
    - Enter `wc -w aup_v1.txt`
    - Verify that you can see the word count of version 1 of the `AUP` policy file.
    - Enter `wc -w aup_v1.txt aup_v2.txt`
    - Verify that you can see the word counts of both versions of the file, as well as a combined total.
    - Enter `diff aup_v1.txt aup_v2.txt` to display the differences between the two files.
    - Verify that you are presented with the differences between each file, as well as suggested actions.
    - The differences are as follows:
    - `33a34,41` means that after `line 33` in the first file (version 1), lines `34–41` from the second file (version 2) need to be added in order for that chunk of text to be the same.
    - The multiple `>` symbols indicate each line that must be added to the first file in order to be the same as the second file.
    - In other words, the HR lead added this entire new section to `version 2` of the policy.
    - `35a44` means that at `line 35` in the first file, `line 44` from the second file needs to be added in order for the text to be the same.
    - In other words, the HR lead added an entry to the revision history explaining her changes.
3. Search the authentication log for failed login attempts.
    - Enter `sudo cat /var/log/secure` to display the contents of the secure log file.
    - Verify that there are many entries in the authentication log.

- Rather than read the entire log or search `term-by-term` for failure entries, you can use `grep` to bring all of the relevant information to the forefront with one command.
- Enter `su - ariley` and provide an incorrect password to simulate an authentication failure.
  - Do not actually sign in. The purpose of this step is to generate a message in the log file.
- Enter `sudo grep failed /var/log/secure` to search for the string failed in the secure log file.
- Verify that you are presented with all lines in the log containing the text string "`failed`".

```
Dec 11 16:52:35 localhost unix_chkpwd[1254]: password check failed for user (root)
Dec 14 13:01:42 localhost unix_chkpwd[1739]: password check failed for user (root)
Dec 14 14:18:45 localhost unix_chkpwd[7351]: password check failed for user (ariley)
Dec 14 14:18:58 localhost sudo: student01 : TTY=pts/0 ; PWD=/home/student01 ; USER=roo
t ; COMMAND=/bin/grep failed /var/log/secure
```

Linking files

Scenario7

```
You've decided to start organizing your backup directory, particularly with regard
to log files. You want to create several subdirectories, each one a category that
can pertain to the backed up logs. For example, you want to organize logs by type
(e.g., authentication logs vs. app logs vs. kernel logs) and the year that they
were generated. However, most logs can apply to multiple categories. Rather than
have two or more distinct copies of each log, you decide to link these files
together so that they're easier to manage.
You also want to be able to quickly access log backups from your home directory.
So, you'll create a link in your home directory to a log in the backup directory.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
        2.3 Given a scenario, create, modify, and redirect files
```

1. Create new log backup directories and move the authentication log to one of them
   - Enter `mkdir /backup/log/auth /backup/log/year` where year refers to the current year.
   - Enter `sudo cp /var/log/secure /backup/log/auth/secure`
   - Enter `cd /backup/log`
2. Create a hard link between the log files
   - Enter `sudo ln auth/secure year/secure`
   - This creates a hard link to the file in the auth directory.
   - Enter `ls -l year` and verify that a file was created in the year directory.
   - Enter `sudo cat year/secure` and verify that its contents are the same as the authentication log.
   - You can run `diff auth/secure year/secure` if you want to be sure.
3. Make a change in one file and see it reflected in the hard link file
   - Enter `sudo nano auth/secure`
   - Press `Enter` to start a new line at the top.
   - Type `BEGIN LOG ##-####` where the hashes are the current month and year.

- For example: `BEGIN LOG 01-2019`
- Press `Ctrl+O` then `ENTER` to save.
- Press `Ctrl+X` to quit.
- Enter `sudo head year/secure` and verify that the header you just added was also added to the hard link file.
- Remove one file and verify that the hard link is still intact
- Enter `sudo rm auth/secure`
- Enter `sudo cat year/secure` and verify that the hard link file's contents are still intact.
- Attempt to create a link from your home directory to a log file in the backup directory
- Enter `cd ~` to return to your home directory.
- Enter `sudo ln /backup/log/year/secure auth-log`
- Verify that the operation failed.
- You cannot create hard links across different file systems, and the home directory and the backup log directory are on different file systems. To get around this, you must create a soft (symbolic) link.
- Create a symbolic link to the log file
- Enter `ln -s /backup/log/year/secure auth-log`
- Enter `sudo cat auth-log` and verify that your link has the expected log contents.
- Delete the original log file and verify that the symbolic link was affected
- Enter `sudo rm /backup/log/year/secure`
- Enter `sudo cat auth-log` and verify that so such file exists.
- Enter `ls -l` and verify that the file is a broken link.
- You should see red text pointing to text with a black background indicating that the link is broken.
- Enter `rm auth-log` to delete the symbolic link.

Manipulating File Output

Scenario8

```
In the past, the IT team has kept an inventory of all laptops issued to employees.
As part of the new roll-out, you'll need to copy this information to a document
that will be stored on a Linux server. The source information isn't formatted very
well, and isn't in any kind of useful order. So, you decide to create a new file
from scratch Afterward, you realize that the person who recorded the information
made a mistake with the format of certain serial numbers. Instead of editing the
file to replace every mistake individually, you'll leverage input and output
redirection to fix the mistakes. Then, you'll output a sorted version that will be
more useful for reference.
You also want to regularly check the contents of the backup directory and place
the results in a continually updated file. You want to be able to see the results
in real-time at the CLI as well, so you'll use the tee command to accomplish both.
Lastly, you'll use piping with grep to further hone your log analysis skills.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
2.3 Given a scenario, create, modify, and redirect files
```

1. Use output redirection to start adding text to the laptop inventory file.
    - Enter `touch laptop_inv.txt` to create a blank file.
    - Enter `echo "User Make Serial No." > laptop_inv.txt`
        - Separate each column by four spaces.
    - Enter `cat laptop_inv.txt` and verify that the text output to the file.
2. Use output redirection to append text to the file.
    - Enter `echo "jsmith Asus S489124" > laptop_inv.txt`
    - Enter `cat laptop_inv.txt` and verify that the header was replaced by this new row.
    - This is because the `>` operator replaces any existing text with the provided string. You need to append that text.
    - Reenter `echo "User Make Serial No." > laptop_inv.txt`
        - Remember, you can press the Up Arrow to return to a command you previously entered.
    - Enter `echo "jsmith Asus S489124" >> laptop_inv.txt`
        - Again, separate each column by four spaces.
    - This time, you're using the append operator `>>`.
    - Verify that the file has both the header and the first row.

```
User Make Serial No.
jsmith Asus S489124
```

3. Use input redirection to replace all instances of a mistyped character in the file.
    - Enter `cp /opt/linuxplus/managing_files_and_directories/laptop_inv.txt laptop_inv.txt`
    - This will update your copy with a filled-in one.
    - Examine the file and verify that the `Asus serial numbers` incorrectly start with the capital letter "`S`".
    - Enter `tr S 5 < laptop_inv.txt`
    - Verify that the instances of "`S`" were replaced with "`5`" and that the file was printed to the CLI.
4. Use both input and output redirection at the same time to create a new file with the corrections.
    - Enter `tr S 5 < laptop_inv.txt > laptop_inv_fix.txt`
    - Examine the corrected file and verify that the appropriate correction was made.
5. Use piping to sort the inventory list without the header.
    - Enter `sort -k1 laptop_inv_fix.txt` to sort the contents.
    - Observe that, just like sorting the software list earlier, the header is included in the sort when it shouldn't be.
    - Enter `tail -n +3 laptop_inv_fix.txt | sort -k1`
    - The `tail -n +3` command outputs everything after and including the third line, which is when the header ends. You are piping the output of this command to the sort command, which takes it as input.

- Verify that the inventory is now sorted by user name, but does not include the header.

```
hroberts    Lenovo  8989090
jcook       Dell    1489284
jsmith      Asus    5489124
kriley      Dell    1390390
lbarnes     Asus    5393892
manderson   Acer    2988481
mstephens   Asus    5737481
nporter     Asus    5892849
rburton     Lenovo  8139003
sarmstrong  Dell    1923843
tlee        Lenovo  8112091
tramirez    Acer    2942349
```

6. Use the `tee` command to redirect output to both the CLI and a file at the same time.
   - Enter `sudo ls -lR /backup > backup_report`
   - Verify that `ls` didn't print its results to the CLI.
   - Enter `sudo ls -lR /backup | tee backup_report`
   - Verify that `ls` did print its results to the CLI.
   - This is because piping the `ls` command to `tee` instead of doing a `stdout redirect` ensures that the results will appear at both the CLI and the specified file.
   - Examine the `backup_report` file and verify that it also lists directory information.
7. Use `grep and cut` together to make log analysis easier.
   - Enter `sudo grep 'password check failed' /var/log/secure`
   - This prints all instances of the text "`password check failed`" from the authentication log. However, it also prints every single part of the line, much of which isn't relevant and just adds to the noise.
   - Enter `sudo cut /var/log/secure -d " " -f5-12`
   - The `cut` command, using the `-d` option, trims each line using a space as a delimiter. The `-f5-12` option specifies the range of the delimiter to extract. So, you're only extracting approximately the middle chunk of each line. However, you're still seeing every line of the log.
   - Enter `sudo grep 'password check failed' /var/log/secure | cut -d " " -f5-12`
   - Verify that you extracted all lines matching the provided string, as well as only the portion of the line that is relevant to your needs.

- The results show the system function that was called, an explanation of the event, as well as the user the event applies to.

06: Managing Kernel Modules

Exploring the Linux Kernel

> Scenario As a system administrator, you may need to troubleshoot issues related to the kernel. So, you want to explore kernel concepts to refresh your knowledge.

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    1.2 Given a scenario, install, configure, and monitor kernel modules
```

1. Log in as `student01` with `Pa22w0rd` as the password.
2. Enter `uname -a` to view information related to the currently running Linux kernel.
3. What is the base version of your currently running kernel according to the `uname` command? ○ 2.4
   ○ 2.6
   ○ 3.4
   ○ 3.10
   ○ 4.18
   Click here for the answer. -> `3.10`
4. True or False? According to the `uname` command, you are running a 32-bit hardware platform. Click here for the answer. -> `False`
5. Which function is associated with the SCI layer of the kernel? ○ Passing requests to device drivers.
   ○ Sending service requests to the kernel.
   ○ Allocating processor time for functions.
   ○ Processing scheduling functions.
   ○ Organizing files on the file system.
   Click here for the answer. -> `Sending service requests to the kernel.`
6. What are the major functions performed by the kernel? (Choose two.) ☐ Kernel initialization
   ☐ `Process management`
   ☐ `Memory management`
   ☐ Module installation
   ☐ Dependency management
   Click here for the answer.
7. Which of the following accurately describe the user space? (Choose two.) ☐ It is the area of the memory where the kernel executes its services.
   ☐ `It is the area of memory in which most high-level software runs.`
   ☐ It is the part of the system that only logged in users can access.
   ☐ `It is the area of memory in which background processes and low-level system`

`libraries run.`
Click here for the answer.

8. What is one disadvantage of a `monolithic kernel` compared to a `microkernel`? ○ Monolithic kernels are slower to access devices.
   ○ `Monolithic kernels are larger and consume more RAM.`
   ○ Monolithic kernels have a smaller kernel space and are less extensible.
   ○ Monolithic kernels can only run the bare minimum software to qualify as a fully functional OS.
   Click here for the answer.

9. True or false? The `Linux` kernel is modular, enabling users to extend its functionality. Click here for the answer. `True`

Installing and Configuring Kernel Modules

> Scenario

```
You want to be able to wirelessly transfer files from the Linux server to your
mobile device. So, you purchase a USB Bluetooth adapter and plug it into an
available port on the server. However, you can't get the adapter to work properly.
After examining the system, you discover that the driver for USB Bluetooth is not
available. So, you'll inspect the kernel and see if you can identify and load the
module that enables this functionality.
```

> Objectives

```
+ Completing this activity will help you to use content examples from the
following syllabus objectives:
  + 1.2 Given a scenario, install, configure, and monitor kernel modules
```

1. `Enter lsmod | less` to examine what modules are currently running.
   - Briefly scan through the list of installed kernel modules.
   - Press `q` to quit.
   - Enter `lsmod | grep bluetooth` to filter the module information for bluetooth content.
   - Verify that there are no results.
   - You don't yet know the name of the relevant module, so this isn't necessarily definitive proof that it isn't loaded.

2. Search for the appropriate module.
   - Enter `uname -r` to retrieve the kernel version of the system.
   - Enter `cd /lib/modules/[kernel version]/kernel/drivers`
     - Remember to use `tab` completion to fill the kernel version automatically.
   - Enter `ls | grep bluetooth` and verify that there is a bluetooth directory.
   - Enter `cd bluetooth` to change to the bluetooth directory.

- Enter `ls` to see the available Bluetooth driver modules.

```
[student01@localhost bluetooth]$ ls
ath3k.ko.xz    btintel.ko.xz      btusb.ko.xz
bcm203x.ko.xz  btmrvl.ko.xz       hci_uart.ko.xz
bfusb.ko.xz    btmrvl_sdio.ko.xz  hci_vhci.ko.xz
bpa10x.ko.xz   btrtl.ko.xz
btbcm.ko.xz    btsdio.ko.xz
```

- Do any of these look like they could be a driver for a USB device that can send and receive Bluetooth signals? Click here for the answer.

  > Answers may vary, but btusb.ko.xz is the most likely candidate.

- Enter `modinfo btusb.ko.xz | less` to learn more about this module.
- Read the information about this module, noting the following:
  - The description indicates that this is a generic Bluetooth USB driver.
  - It has many different aliases that aren't very user friendly.
  - It depends on several other modules.
- Press `q` to quit.

3. Configure an alias for the Bluetooth USB module.

- Enter `cd /etc/modprobe.d` to change to the `modprobe.d directory`.
- Enter `sudo vim btusb.conf` to create a configuration file for the module.
- Create a new empty file by using `Vim`, and then type `alias blue btusb` as the first line.
- Save and close the file.

4. Insert the Bluetooth USB module into the running kernel.

- Enter `sudo depmod` to update the dependencies database.
- Enter `sudo modprobe -a blue`
- Enter `lsmod | grep btusb`
- Verify that the `btusb` module is listed, indicating that it is inserted into the kernel.
- Notice that there are other modules that begin with `bt`, as well as a module called `bluetooth`. Why were these added to the kernel as well? Click here for the answer.

  > These are modules that btusb depends on in order to function. The modprobe command automatically installs dependent modules when necessary.

Monitoring Kernel Modules

> Scenario

Now that you installed the USB Bluetooth module, you want to make sure it was successfully loaded by the kernel and that there are no errors. You also want to identify your kernel version details in case you need to reference it during troubleshooting.

Objectives_

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   + 1.2 Given a scenario, install, configure, and monitor kernel modules
```

1. Enter `cat /proc/version` and use the result to answer the following questions.
    - When was the kernel last compiled? Click here for the answer.

      > Answers may vary, but the version used to develop this course was compiled on November 8th of 2018

    - What version of the GCC is your kernel running? Click here for the answer.

      > Answers may vary depending on when the kernel was compiled. For the kernel version used to develop this course, the GCC version is 4.8.

    - Why might this information be useful? Click here for the answer.

      > Answers may vary, but validating the kernel version and related information can help you diagnose issues that apply to specific versions, such as incompatible software.

    - Enter `dmesg -h` to examine the kernel message help.
    - Note the different facilities and log levels available. Examples include warn, err, notice, etc.
    - Enter `dmesg -H`
        - Don't forget to use the man pages to discover the meaning of the different options for commands. What is the meaning of the `-H` option for `dmesg`?
    - Verify that you can navigate through many pages of kernel messages.
    - Not all of the information here will be useful to you, so you'll need to filter what you're looking for.
    - Press `q`.

2. Filter the kernel message buffer for more useful messages.
    - Enter `dmesg -H -l warn`
    - Verify that the results have been filtered.
    - All of these messages are marked as warning conditions. These don't necessarily indicate errors but call attention to behavior that might be worth checking.
    - If necessary, press `q`.
    - Enter `dmesg -H -l err`
    - These messages do indicate errors. You might not have any results, which means the kernel hasn't recorded any errors thus far.
    - If necessary, press `q`.
    - Enter `dmesg -H | grep usb` to search the kernel message buffer for evidence of USB drivers being loaded.

3. Examine the results.
    - The kernel records when USB storages devices are found and when drivers are registered. It also identifies when input devices that use USB are found—like a mouse, keyboard, webcam, etc.

- Enter `dmesg -H | grep btusb` to use `grep` to search for Bluetooth USB information.
- Verify that the kernel is reporting that a new interface driver was registered for the `btusb` module you installed earlier.

```
[student01@localhost modprobe.d]$ dmesg -H | grep btusb
[  +0.001415] usbcore: registered new interface driver btusb
[  +0.000052]  ath9k_hw ath mac80211 iTCO_wdt iTCO_vendor_sup
uvcvideo snd_hda_codec_realtek videobuf2_vmalloc videobuf2_me
f2_core videodev snd_hda_codec_hdmi snd_hda_codec_generic i2c
```

Managing The Linux Boot Process

Creating an initrd Image

Scenario

```
As part of your server infrastructure, you plan on having some systems boot from
an NFS share. The kernel in the deployed systems doesn't have an NFS module.
Without this, your systems cannot mount an NFS share as the root file system. So,
you need to create a new initrd image so that the kernel can successfully mount
the share. First, however, you'll establish a baseline image that other images can
build off of.
```

Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 1.1 Explain the Linux boot process
  - 3.3 Summarize security best practices in a Linux environment

1. Create a new `initrd` image.

   - Log in as `student01` with `Pa22w0rd` as the password.
   - Enter `uname -r` to identify the current kernel.
   - Enter `sudo mkinitrd -v /boot/initrd-$(uname -r).img $(uname -r)`
     - `$(uname -r)` substitutes the name of the kernel in this command.
   - Examine the verbose output from mkinitrd noting the various kernel modules that are included in the initrd image by default.
   - Enter `ls -l /boot` and verify that your new initrd image was created.
   - The image should be named `initrd-.img` and should have been last modified on today's date.

2. Create an `initrd` image with an NFS module installed.

   - Enter `sudo mkinitrd -v --with=nfsv4 /boot/initrd-$(uname -r)-nfs.img $(uname -r)`
     - Check your syntax before you hit enter. Also, do not forget that Tab completion can make your life a great deal easier.
   - Enter `ls -l /boot` and verify your new NFS image was created.
   - Examine the file sizes for both `initrd` images (the base image and the NFS image) and verify that the NFS image is larger. This suggests that the additional NFS module was loaded into the image, as intended.

```
*** Including module: microcode_ctl-fw_dir_override ***
  microcode_ctl module: mangling fw_dir
    microcode_ctl: reset fw_dir to "/lib/firmware/updates /lib/firmware"
    microcode_ctl: processing data directory  "/usr/share/microcode_ctl/ucode_with_caveats/intel"...
intel: model '', path ' intel-ucode/*', kvers ''
intel: blacklist ''
    microcode_ctl: intel: Host-Only mode is enabled and ucode name does not match the expected one, skipping caveat ("06-4f-01"
not in " intel-ucode/*")
    microcode_ctl: processing data directory  "/usr/share/microcode_ctl/ucode_with_caveats/intel-06-4f-01"...
intel-06-4f-01: model 'GenuineIntel 06-4f-01', path ' intel-ucode/06-4f-01', kvers ' 4.17.0 3.10.0-894 3.10.0-862.6.1 3.10.0-693
.35.1 3.10.0-514.52.1 3.10.0-327.70.1 2.6.32-754.1.1 2.6.32-573.58.1 2.6.32-504.71.1 2.6.32-431.90.1 2.6.32-358.90.1'
intel-06-4f-01: blacklist ''
intel-06-4f-01: caveat is disabled in configuration
    microcode_ctl: kernel version "3.10.0-957.el7.x86_64" failed early load check for "intel-06-4f-01", skipping
    microcode_ctl: final fw_dir: "/lib/firmware/updates /lib/firmware"
*** Including module: shutdown ***
*** Including modules done ***
*** Installing kernel module dependencies and firmware ***
*** Installing kernel module dependencies and firmware done ***
*** Resolving executable dependencies ***
*** Resolving executable dependencies done***
*** Hardlinking files ***
*** Hardlinking files done ***
*** Stripping files ***
*** Stripping files done ***
*** Generating early-microcode cpio image contents ***
*** Constructing GenuineIntel.bin ****
*** No early-microcode cpio image needed ***
*** Store current command line parameters ***
*** Creating image file ***
*** Creating image file done ***
*** Creating initramfs image file '/boot/initrd-3.10.0-957.el7.x86_64-nfs.img' done ***
[student01@localhost ~]$ ls -l /boot
total 195940
-rw-r--r--. 1 root root   151918 Nov  8  2018 config-3.10.0-957.el7.x86_64
drwx------. 3 root root    16384 Dec 31  1969 efi
drwxr-xr-x. 2 root root       27 Jan 11  2019 grub
drwx------. 2 root root       21 Jan 11  2019 grub2
-rw-------. 1 root root 73996789 Jan 11  2019 initramfs-0-rescue-f6f7a37d52454c709b242c2d60ac77f9.img
-rw-------. 1 root root 32007830 Jan 11  2019 initramfs-3.10.0-957.el7.x86_64.img
-rw-------. 1 root root 13646428 Jan 11  2019 initramfs-3.10.0-957.el7.x86_64kdump.img
-rw-------. 1 root root 31594808 May 16 11:16 initrd-3.10.0-957.el7.x86_64.img
-rw-------. 1 root root 32063922 May 16 11:18 initrd-3.10.0-957.el7.x86_64-nfs.img
-rw-r--r--. 1 root root   314036 Nov  8  2018 symvers-3.10.0-957.el7.x86_64.gz
-rw-------. 1 root root  3543471 Nov  8  2018 System.map-3.10.0-957.el7.x86_64
-rwxr-xr-x. 1 root root  6639904 Jan 11  2019 vmlinuz-0-rescue-f6f7a37d52454c709b242c2d60ac77f9
-rwxr-xr-x. 1 root root  6639904 Nov  8  2018 vmlinuz-3.10.0-957.el7.x86_64
[student01@localhost ~]$
```

Configuring GRUB 2

- Scenario

> Some of your fellow administrators are claiming that their Linux servers aren't booting properly. You are assigned to the task of troubleshooting these issues. You find that someone has modified the settings in the boot loader because there is no password protection. After correcting the boot configuration, you decide to protect GRUB 2 with a password so that only authorized users can modify it.

Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 1.1 Explain the Linux boot process

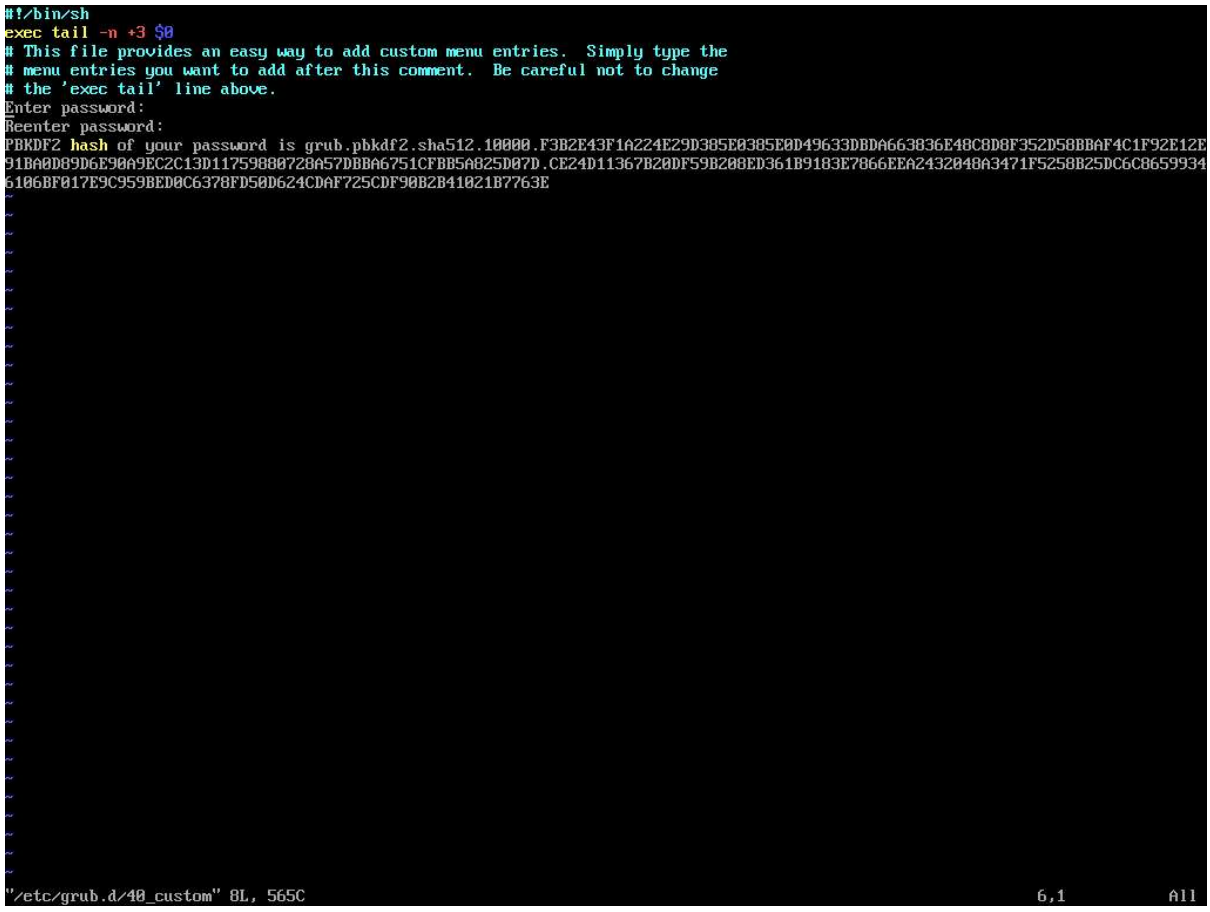
1. Verify that GRUB 2 is installed.
   - Enter `sudo ls -l /boot/efi/EFI/centos` to display the contents of the directory.
   - Verify that `grub.cfg` exists in this directory.
   - The presence of this file usually indicates that `GRUB 2` is successfully installed on the EFI system partition.
   - Enter `sudo cat /boot/efi/EFI/centos/grub.cfg` and verify that the configuration file is populated.

```
[student01@localhost modprobe.d]$ sudo cat /boot/efi/EFI/centos/grub.cfg
#
# DO NOT EDIT THIS FILE
#
# It is automatically generated by grub2-mkconfig using templates
# from /etc/grub.d and settings from /etc/default/grub
#

### BEGIN /etc/grub.d/00_header ###
set pager=1

if [ -s $prefix/grubenv ]; then
  load_env
fi
```

2. Create a password to lock the `GRUB 2` configuration with.
    - Enter `sudo grub2-mkpasswd-pbkdf2 | sudo tee -a /etc/grub.d/40_custom`
    - You're redirecting the output to the custom configuration file. You'll clean up this file shortly.
    - Enter `Pa22w0rd` as the password.
    - Reenter the same password.
    - Verify that the `PBKDF2` password is generated.
    - `PBKDF2` uses a cryptographic technique called hashing to protect the password in storage.
3. Adjust the custom `GRUB 2` configuration file to require your password.
    - Using `sudo`, open `/etc/grub.d/40_custom` in the text editor of your choice.



    - Move the cursor to the line that says "`Enter password:`" and cut this entire line.
    - Cut the line after it that shows the `reenter password prompt`.

- From the "`PBKDF2`" line, delete the string of text that says "`PBKDF2 hash of your password is`".
- On the same line, replace the text you deleted with `password_pbkdf2 student01`

- Insert a new line above this that says:
- `set superusers="student01"`

- Save and close the file.

4. Update the main GRUB 2 configuration file to apply your changes.

   - Enter `sudo grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg` to cause grub to create a new configuration file.
   - There may be an I/O error message for the `fd0` (floppy drive) device. This will not affect the boot process. Verify that no other errors are returned and that the "`done`" message is displayed.
   - This indicates that the new `GRUB 2` configuration file has been generated successfully.

5. Test the password from the GRUB 2 boot menu.

   - Enter `reboot` to restart the server.
   - On the `GRUB 2` boot menu screen, press `Esc` to stop the default selection timer.
   - Press `e` to edit the GRUB 2 configuration.
   - At the `Enter username` prompt, enter the account name `student01`.
     - Input your user name and password very carefully, as you will be unable to edit any mistakes.
   - At the `Enter password` prompt, enter `Pa22w0rd`
   - Verify that you can see the `GRUB 2` configuration on the screen.

- Press `Esc` to exit editing mode.
- Press `Enter` to boot back into the default selection.
- Log back in as your student account.

08: Managing System Components

Configuring Localization Options

Scenario

```
One of your colleagues is located remotely—in London, England. Just like you, he
needs to be able to log in to Develetech's Linux servers in order to administrate
them. The server he needs to remotely administrate is located in the US, even
though it primarily services users in Great Britain. So, you'll set this server to
use the time zone in London, as well as change the language and keyboard layout
settings to those of Great Britain. This will make it easier for your English
colleague to work within the environment and for the server to operate within the
correct time zone.
```

Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: 1.6 Given a scenario, configure localization options

1. Retrieve your system's current date and time information.
    - Log in as `student01` with `Pa22w0rd` as the password.
    - Enter `timedatectl` to display time configuration information.
    - Verify that you are given information such as:

Index	Time
1	The local time.
2	The universal time.
3	The real-time clock (RTC) time (i.e., hardware clock).
4	The time zone.
5	Network Time Protocol (NTP) information.
6	Daylight savings time (DST) information.

2. Find the time zone for London.
    - Enter `timedatectl list-timezones` to list the time zones.
    - Verify that there are several pages of time zones available.
    - Time zones are categorized by global region, then typically by city or small nation. This information is pulled from the time zone files and directories in `/usr/share/zoneinfo`
    - Press `q` to quit and return to the prompt.
    - Enter `timedatectl list-timezones | grep London` to filter the results.
    - The relevant time zone is in the format Europe/London.

- Enter `sudo timedatectl set-timezone Europe/London` to change the time zone to London's current time zone.
- Enter `timedatectl` again to display the updated time configuration information.
- Verify that the time zone has changed and that the local time reflects this change.
- The time zone that is set will depend on the time of year. From the last Sunday in March to the last Sunday in October, the time zone will be `British Summer Time (BST)`. The rest of the year, London is on `Greenwich Mean Time (GMT)`, otherwise referred to as `UTC`.
- Verify that the universal time is either the same as the local time or is one hour behind, depending on the time of year.
- The universal time is synonymous with `GMT/UTC` and is used as a global reference point.
- Examine the `RTC` time.
- This is the hardware clock, and it is set by the OS. Many Linux distros set this to `UTC` by default, including `CentOS`. You'll leave this as-is.
- Enter `date` to confirm the date and time on the system.

3. Find the appropriate locale settings for Great Britain.

- Enter `localectl status` and note your system's current language locale and keyboard layout.
  - Take note of these values if your locale and keyboard layout are not US. You will need to revert to these values at the end of the activity.
- Enter `localectl list-locales` to display available locale information.
- Page through the list of available locales until you get to the locales that start with `en_ (English language)`.
- Find the `en_GB.utf8 locale`.
- This is a `locale for Great Britain` that uses `UTF-8 encoding`.
- Press `q` to quit.
- Enter `localectl list-keymaps` to display keyboard mapping information.
- Verify that you can find a keyboard layout named `gb` indicating Great Britain.

4. Configure the appropriate locale settings for Great Britain.

- Enter `sudo localectl set-locale "LANG=en_GB.utf8"`
- Enter `sudo localectl set-keymap gb`
- Enter `localectl status` and verify that the language locale and keyboard layout are both set to Great Britain.
- On your keyboard, press the Backslash key and verify that it types a number symbol `(#)`.
- This is due to layout differences between `US` and `GB/UK` keyboards.
  - This will, of course, only work if you're using a US keyboard.

5. For classroom purposes, revert the locale settings.

- Enter `sudo localectl set-locale "LANG=en_US.utf8"`
  - Press the Up Arrow until you retrieve the command you used to set the locale to Great Britain. Then you can just replace the text.
  - If your original language and keyboard layout are something other than US, you will need to enter your original values instead.
- Enter `sudo localectl set-keymap us`
- Enter `localectl status` and verify that the original locale options are set.

Configuring GUIs

Scenario2

```
The CLI has been adequate so far, but many of your colleagues would be more
comfortable working in a visual environment. A GUI is also necessary for easily
browsing the web and viewing media like images and video. Most of your colleagues
prefer to work with GNOME, the default desktop environment, whereas others prefer
a customized version of KDE. So, you'll start by configuring KDE's layout options
to align with those users' preferences. Then, you'll get accustomed to navigating
through GNOME, the environment you yourself will be using. You also need to
configure some accessibility options in GNOME for users who have visual and manual
dexterity impairments.
```

Objectives2

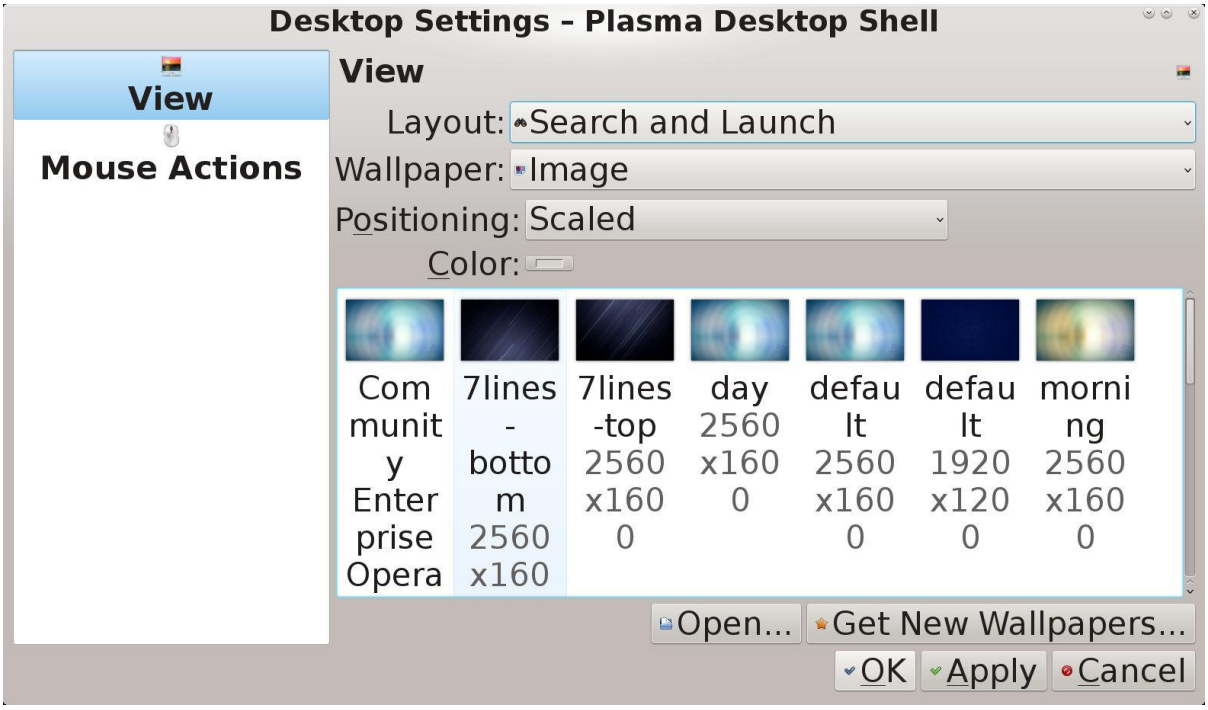
```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    2.8 Compare and contrast Linux graphical user interfaces
```

1. Switch to the GUI, then log in to KDE.
    - Enter `sudo systemctl isolate graphical.target` to launch the graphical user interface.
        - Recall that many Linux servers are run with no graphical user interface (`GUI`). The `GUI` can be a drain on system resources.
    - Verify that you are presented with a graphical login screen.

- Select `student01`.
- To the left of the Sign In button, select the Settings gear icon.
- Select `KDE Plasma Workspace`.
- Enter your password and select Sign In.
  - The two most common `GUIs` for `Linux` are `GNOME` and `KDE`. There are many others available, however.

2. Configure desktop settings for `KDE`.

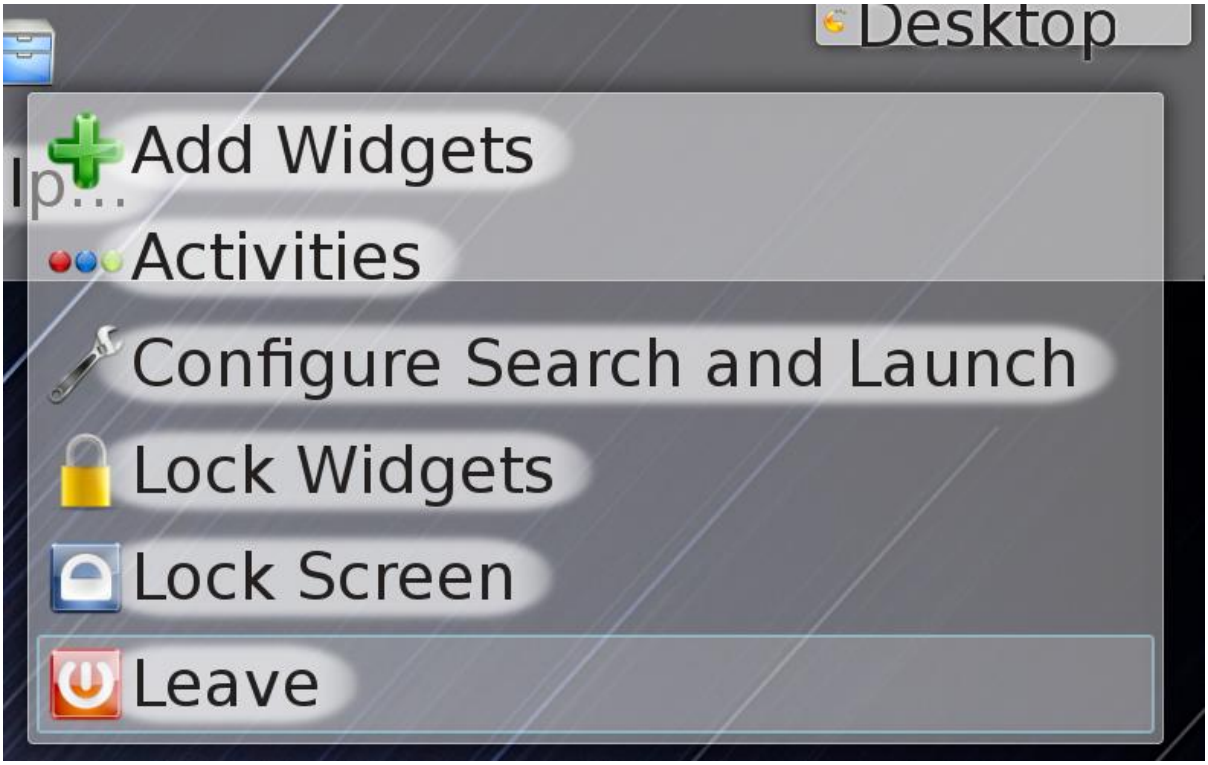
- On the desktop, right-click and select `Default Desktop Settings`.
- In the Desktop Settings - `Plasma Desktop Shell window,` in the *left pane*, verify that **View** is selected.
- From the **Layout drop-down list**, select `Search and Launch.`
- In the *images* section, select `7lines-bottom` from the thumbnails list.



- Select OK to apply the settings and close the `Desktop Settings - Plasma Desktop Shell window`.
- Examine the new layout of the desktop environment.

3. Switch to ``GNOME.

- From the `top-right of the desktop`, select the `Desktop menu`, then select `Leave`.



- Select `Logout`.
- Select `student01`.
- To the `left` of the `Sign In button`, select the `Settings icon`.
- Select `GNOME Classic`.
- Sign in using your `password`.
- If displayed, go through the preliminary setup options.

- On the `Welcome screen`, select `Next`.
- On the `Typing screen`, select `Next`.
- On the `Network screen`, select `Skip`.
- On the `Privacy screen`, select `Next`.
- In the dialog box, select **Deny Access**.
- On the *Online Accounts screen*, select `Skip`.
- On the *Ready to Go screen*, select `Start` using `CentOS Linux`.
- Close the *Getting Started window*.
- Examine the desktop and note that `GNOME` has a different look and feel than `KDE`.

4. Navigate the `GNOME` desktop and open an application.

- From the desktop menu, select `Applications→Favorites→Files`.
- Verify that you are in your `home` directory.
- Double-click the `backup_report file` to open it in the default GUI text editor.
- Make a change to the file, then select `Save`.
- *Close* the text editor.
- *Close* the file browser.

5. Enable accessibility settings in `GNOME` for users with visual and manual dexterity impairments.

- Select `Applications→System Tools→Settings`.
- From the navigation pane on the left, select `Universal Access`.
- In the `Seeing section`, slide the **High Contrast slider to On**.
- In the Pointing & Clicking section, select `Click Assist`. In the `Click Assist dialog box`, slide the `Hover Click slider` to `On`. In the `Hover Click dialog box`, select `Double Click`.
- Close all open dialog boxes.

6. Open a `terminal`, then revert the accessibility changes.

- From the desktop menu, point to (but don't click) `Applications→Favorites→Terminal`. The `Click Assist` feature will "click" the menu options for you.
- From the top-right of the desktop taskbar, select the Universal Access icon  , then slide `High Contrast to Off`.
- Select `Applications→System Tools→Settings`. Select `Click Assist`. In the `Click Assist` dialog box, slide the Hover Click slider to Off.
- Keep the terminal window open.

Managing Services

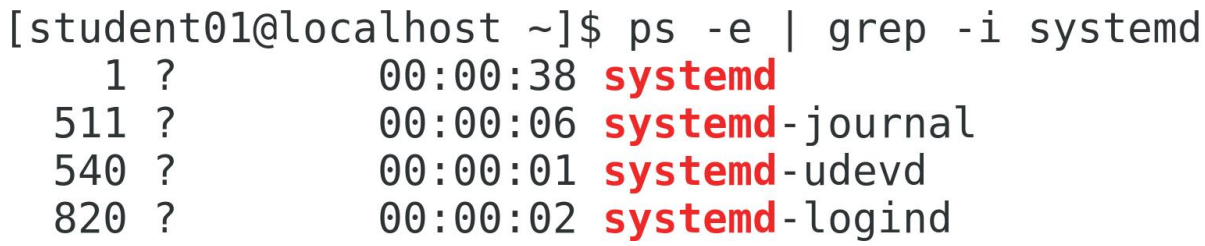
Scenario3

```
As a Linux administrator at Develetech, you know that you will be implementing,
managing, and reconfiguring different services. You'll be leveraging systemd, and
in particular, the systemctl command and its associated subcommands, to manage
these services. You decide to start by switching targets from CLI to GUI, and then
making the default target GUI so that users will always boot into that environment
by default. Then, you'll practice managing the SSH and firewall services by
```

```
putting them through the service management lifecycle of starting, stopping,
enabling, and disabling them.
```

Objectives3

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    2.4 Given a scenario, manage services
```

1. Verify that your system is using systemd and not the older `SysVinit` method.
    - In the terminal window, enter `ps -e | grep -i init` to check for the `init` process.
    - Verify that the `init` process was not found.
    - Enter `ps -e | grep -i systemd` to check for the `systemd` process.
    - Verify that the `systemd` process was found and has a `process ID of 1`.
    - 

        - If `PID 1` is `init`, then the system is using the older `SysVinit` startup method. If `PID 1` is `systemd`, then the system is using the newer method.

2. View the target files that specify the services that will start when the system starts
    - Enter `cat /usr/lib/systemd/system/multi-user.target`
    - Observe that the `multi-user.target` requires the `basic.target–i.e.`, the target files build upon each other.
    - Enter `cat /usr/lib/systemd/system/graphical.target`
    - Observe that the `graphical.target` requires the `multi-user.target–this` further illustrates how the target files build on each other. In addition, the `graphical.target` calls or "wants" the `display-manager.service`, which initiates the GUI.
    - Enter `systemctl --type=service` to view the current target's services.
    - Press `q` when you're finished.

3. Switch between the `CLI target` and the `GUI target`, then set the `GUI target` as the default.
    - Enter `sudo systemctl isolate multi-user.target` to switch back to the command-line interface.
    - Sign in as `student01` using `Pa22w0rd` as the password.
    - Enter `sudo systemctl isolate graphical.target` to switch to the graphical user interface.
    - Sign in as `student01` and open a terminal.
    - Enter `sudo systemctl set-default graphical.target` to set the GUI as the default environment.

4. Examine the `systemctl` subcommands.
    - Type `systemctl` and then type a `space`, and then press `Tab` twice.
    - You can use this trick with some commands to list all of their available subcommands.
        - Be sure to add a `space` after the command and before pressing `Tab`.
    - Note the `stop`, `start`, `restart`, `status`, `enable`, and `disable subcommands` in particular.

5. Manage the `SSH service` on your server.
    - Enter `sudo systemctl status sshd.service` to check the status of `sshd`.
    - Verify that the `sshd` service is running.
    - Enter `sudo systemctl stop sshd.service` to stop the SSH service.
    - Verify that the `sshd service` is stopped.
    - Enter `sudo systemctl start sshd.service` to start the `sshd` service again, then check its status to ensure it is running.

```
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor
preset: enabled)
   Active: active (running) since Tue 2018-12-11 18:31:12 GMT; 3 days ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 1346 (sshd)
    Tasks: 1
   CGroup: /system.slice/sshd.service
           └─1346 /usr/sbin/sshd -D
```

```
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor
preset: enabled)
   Active: inactive (dead) since Fri 2018-12-14 19:48:49 GMT; 4s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 1346 ExecStart=/usr/sbin/sshd -D $OPTIONS (code=exited, status
=0/SUCCESS)
 Main PID: 1346 (code=exited, status=0/SUCCESS)
```

6. Disable, and then re-enable, the `firewalld` service.
    - Enter `sudo systemctl status firewalld.service` to verify the status of the `firewalld service`.
    - Verify that the `firewalld service` is running.
    - Enter `sudo systemctl disable firewalld.service` to disable the `firewalld` service.
    - Verify that the `firewalld service` is still running.
    - The `enable` and `disable` subcommands do not affect the current status of the service, but rather the startup status.
    - Reboot the server, log back in to the GUI with your `student01` account, and verify that the `firewalld` service is not running.
    - Start the `firewalld` service again.
    - Use the `systemctl` command to enable the `firewalld` service.

Troubleshooting Process Issues

Scenario 4

```
Some users have complained that processes on the Linux server are taking longer
than normal to complete. You discover several processes that are not needed are
still running and were never successfully terminated. You need to manage the
system processes and the processes issued by other users. In addition, you'll see
if there are any problem processes that are consuming too many resources or are
causing delays in the boot process.
```

Objectives 4

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    4.2 Given a scenario, analyze system properties in order to optimize
performance
```

1. Obj 4

    - Enter `ps` to list only the processes running on the current terminal.
    - Verify that only the processes started by your account are listed.
    - Enter `ps -e` to list all the processes running on the system.
    - Verify that more processes are listed as compared to the output of the standard ps command.

2. Discover the process ID number of a process for which you know the name.

    - Enter pgrep sshd to display the `PID` for the `sshd service`.
    - Note the process ID number of the `sshd service`.

3. Issue a background command.

    - Enter `sleep 300 &` to pause the system for 300 seconds.
    - Enter the `PID` of the `sleep 300 &` command in the text box below:
    - Enter `ps` to display the processes running under your account.
    - Verify that the `sleep` command is in the list of running processes.

4. Terminate the `sleep` command.

    - Enter `kill <sleep>` by using the `PID` for the sleep command.
    - Enter `ps` to check the status of the sleep command.
    - Verify that the sleep command is not in the list of running processes.

5. Explore more process information with the top command.

    - Enter `top` to open the process management tool.
    - Press `M` to reorganize the output by **memory usage**.
    - Press `P` to reorganize the output by **CPU usage**.
    - Press `q` to **exit the top program**.
    - Discover what files are open, and which processes opened them.
    - Enter `lsof`

- Enter `lsof -u student01` to see files opened by a specific user.

6. View boot performance information.

- Enter `systemd-analyze`
- The results of the `systemd-analyze` command break the startup process into three parts: **how long it took the kernel to start**, **how long it took the `initrd` image to load**, and **how long user startup applications and services took to start**. The command also shows the total amount of time the startup took. This information can be used in troubleshooting long startup times.
- Enter `systemd-analyze blame` to see which processes take the longest to start during boot.
- Press `q`.

Prioritizing Processes

Scenario 5

```
You want to back up the local copy of the /etc/ configuration directory. You
expect the copying process to be time-consuming and to continue after you log out
of your system. You decide to increase the priority of the process to ensure that
it is completed on time.
```

Objectives 5

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    4.2 Given a scenario, analyze system properties in order to optimize
performance
```

1. View the nice values of running processes.

- Enter `ps xl | less` to view all processes run by users.
- Examine the processes that have the highest nice value.
  - The nice value defines how much attention the process will receive. The scale is `-20 to 19`, with **-20 being the highest possible priority**. Most processes launch with a nice value of `0`.
- Press `Page Down` until you reach the end of the entire list.
- Press `q` to exit the list.

2. Issue the command to copy files as a background process.

- Enter `for i in {1..100}; do sudo cp -R /etc /backup/sys; done &` to begin the copy process. This issues the copy command 100 times to simulate a long-running task.
  - Double-check your syntax before running the command.
- Verify that the `PID` and the job number are displayed.
- Enter the `PID` in the text box below:

3. Renice the `copy` process by using the `top` command.

    - Enter `sudo top` to open the process management tool.
    - Press `r` to *renice* a process from within top.
    - Enter the `process ID <copy>` - the copy operation you noted previously.
    - Enter `-15` to specify the nice value.
    - Press `q` to exit the process list.
    - Enter `ls /backup/sys`
    - Verify that the files from the `/etc` directory are listed, indicating that the copy process was successful.

Troubleshooting CPU and Memory Issues

Scenario 6

```
You want to identify some basic tools to help manage system components.
Specifically, you'll review processor and memory usage to see if the results match
expected performance.
```

Objectives 6

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    4.1 Given a scenario, analyze system properties and remediate accordingly
```

1. Gather information on the CPU.

    - Enter `less /proc/cpuinfo` to *display processor information*.
    - Press `q` to *quit*.
    - Enter `uptime` to see how long the system has been up and view basic performance information on the CPU.

2. Use `sar` to gather system information.

    - Enter `sar -u` to retrieve basic performance information.
    - Enter `sar 2 6` to retrieve information *every two seconds*, for a *total of six queries*.
    - Enter `sar -S` to retrieve *swap space usage information*.

3. Gather information on system memory.

    - Enter `less /proc/meminfo` to *display memory information*.
    - Press `q` to quit.
    - Enter `free` to *gather basic memory usage information*.
    - Enter `free -m` to see the *memory usage measured in megabytes*.
    - Enter `free -h` to see *memory usage in human-readable format*.

4. Use the `vmstat` command to gather virtual memory usage information.

- Enter `vmstat 5 3` and wait for the report to finish.
- Enter `vmstat -d 5 3` to see the information organized on a *per-storage device basis*.

09: Managing Devices

Configuring a Virtual (PDF) Printer

Scenario

```
HR wants to distribute the acceptable use policy (AUP) to employees at Develetech
in both hardcopy and electronic form. Right now, you don't have an actual printer
connected to your Linux system, but you can still print the AUP text file to a
PDF, which is more suitable than a raw text file for distribution purposes. Before
you can create the PDF, you'll need to set up a virtual printer.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    2.7 Explain the use and operation of Linux devices
    4.4 Given a scenario, analyze and troubleshoot application and hardware issues
```

1. Examine the current list of printers
    - Log in as `student01` with `Pa22w0rd` as the password.
    - From the Desktop, select `Applications→System Tools→Settings.`
    - From the navigation menu, select Devices.
    - Select `Printers`.
    - Verify that no printers are currently listed.
    - Keep this window open.
2. Install the Cups-PDF package
    - In a terminal, enter `sudo yum -y install epel-release cups-pdf`

      You may need to issue this command twice in order to successfully download the package.

      You may receive a repeating messages that says an "`Existing lock /var/yum/yum.pid`: another copy is running." Open a second tab in the terminal (or a second instance of a terminal), and then enter the following command:

      ```
      sudo systemctl kill packagekit
      ```
3. Make the `Cups-PDF` printer your default printer
    - Return to the Settings window and verify that `Cups-PDF` is listed in the printers list. If it is not listed, repeat the install command you just entered.

- Select `Unlock`, then enter the `root` password.
- Next to the Cups-PDF printer, select the options gear icon, then select Use Printer by Default.
- Close the `Settings` window.

4. Print a text file to PDF

- Open a terminal window and verify that you are in your home directory.
- Enter `lpr policies/aup_v2.txt`
- Verify that a printing notification pops up from the desktop.
- On the desktop, double-click `aup_v2.pdf` to open it.
- Close the *PDF viewer* when you're done.

Monitoring Devices

Scenario

```
As part of your routine system administration tasks, you need to track the devices
used on all the computers on the network and maintain a list of hardware resources
that are in use.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    2.7 Explain the use and operation of Linux devices
    4.4 Given a scenario, analyze and troubleshoot application and hardware issues
```

1. Monitor any PCI devices that are connected to the system.

- In a terminal window, enter `lspci`
- Examine the brief list of hardware devices that are connected to **PCI buses**.
- Each line lists the `PCI slot a device` is connected to, as well as the vendor and product model of the device.
- Enter `sudo lspci -v` to view more information about each device.
- Verify that you can see attributes of each device, such as:
  - Its **vendor and product model**.
  - Its `I/O ports`.
  - Its various capabilities.
  - The **kernel modules and drivers** it uses.
  - In the virtual lab environment no USB drivers are loaded. In a real, physical environment, you'd also be able to enter the `lsusb` command to see USB devices on your system.

2. Monitor a print job.

- Enter `base64 /dev/urandom | head -c 10000000 > printfile.txt`
  - There are `7 zeros`.

- This will create a text file `10 MB` in size using random data encoded in readable text (`Base64`). This file is large enough to take some time to print, so you'll have a chance to monitor it in the queue.

3. Enter `lpr printfile.txt` to start a print job.

   - Enter `lpq` and note that you can see the print job in the queue, including information such as:
     - Its rank (status).
     - Who owns the print job.
     - The number of the job.
     - What file(s) are being printed.
     - The total size of the request.
   - Allow the print job to finish.

10: Managing Networking

Configuring the Server's Network Identity

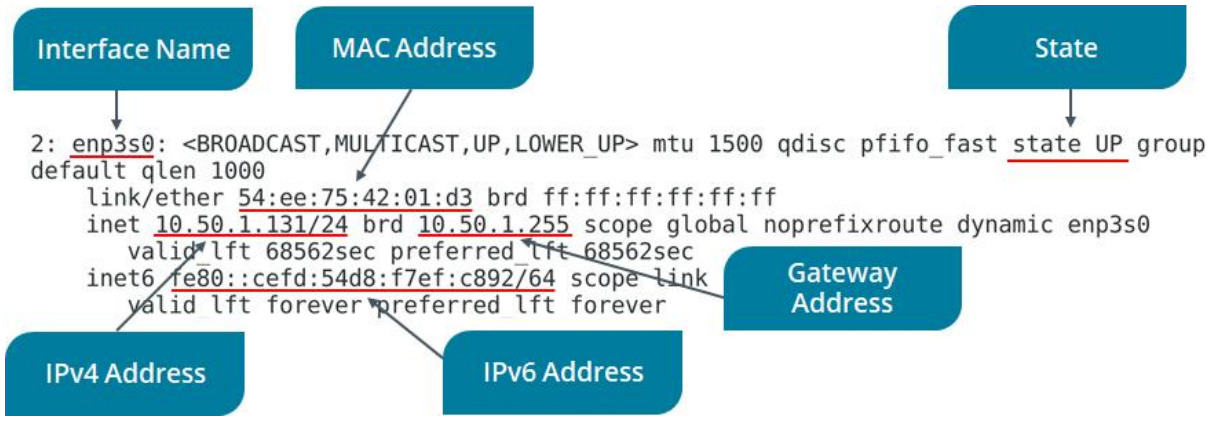
Scenario

```
You need to ensure the system's hostname and IP address configuration is correct.
You also need to be able to configure network settings whether or not a GUI is
installed. You will configure the system with both a static IP address and a
dynamic IP address.
```

> Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   1.3 Given a scenario, configure and verify network connection parameters
   2.7 Explain the use and operation of Linux devices
```

1. Set the server's hostname
    - Log in as `student01` with `Pa22w0rd` as the password.
    - In a terminal window, enter `hostname` to view the system's current `hostname.`
    - Enter `nmcli general hostname` to use a different command to view the system's current `hostname`.
    - Enter `sudo hostnamectl set-hostname server01` to configure a new hostname.
    - Enter `sudo systemctl restart systemd-hostnamed` to restart the service, making the change persistent.
        - Recall that you will almost always have to restart services for changes to be implemented.
    - Verify that your system's `hostname` has changed.
2. Verify the current IP address configuration of the server
    - Enter `man ifconfig` and note the man page entry that indicates the tool is deprecated (retired).
    - Press `q` to quit.
    - Type `ip` (don't press Enter), add a `space`, then press `Tab` twice to see a list of available subcommands.
        - Be sure to include a space before pressing `Tab` twice. This tip takes advantage of tab completion. It displays the subcommands associated with the `ip` command.
    - Enter `ip addr` to display information about available network interfaces.
    - On `CentOS 7`, the main Ethernet device you should use will usually be named in the format `ens##` or `enp#s#`. For the following steps, make sure you're using the **Ethernet interface** identified with this name, and not the **loopback adapter** or a *wireless LAN adapter*.
    - Enter the interface name in the following text box - make sure you record the interface name, such as `ens32`, not the `IP or MAC address`:
    - Enter `ip addr show <devID>` to display the information for a specific interface.



    - If there is an error, make sure you are using the interface name from the output of the previous step. For example, the interface name value might be `ens32`
    - One of the first steps in networking troubleshooting is to verify the current IP address configuration. Therefore, the ip command will be essential to your network troubleshooting process.

3. Display network information by using `nmcli`
    - Enter `nmcli general status` to view the current network connectivity status according to `NetworkManager`.
    - Enter `nmcli` connection show to see the `connection name, UUID, type, and device ID` for each interface.
        - On this host, the connection name and device ID are identical. It is possible to configure different connection profiles that use the same device (`NIC`). For example, you could create a static IP connection profile and one that uses DHCP and switch between them as needed.
4. Disable and enable a `NIC` using `nmcli`
    - Enter `nmcli con down <devID>` to stop the interface, making it inactive.
    - Enter `nmcli device status` to view the current status.
    - Enter `nmcli con up <devID>` to re-enable the interface, making it active.
    - Enter `nmcli device status` to view the current status.
5. Configure the system with a static IP address using `nmcli`
    - Enter `ip addr show <devID>` to view the current IP address.
    - Enter `nmcli con edit <devID>` to edit the interface's IP address configuration.
    - Enter `set ipv4.addresses 10.50.1.101/24` to set the static IP address at the `nmcli` prompt.
    - Press `Enter` to set `ipv4.method` to manual
    - Enter `save at the nmcli prompt`.
    - Enter `quit at the nmcli prompt`.
    - Enter `nmcli con down <devID>`
    - Enter `nmcli con up <devID>` to reset the connection.
    - Enter `ip addr show <devID>` to confirm the static IP address is configured.

```
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 54:ee:75:42:01:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.50.1.101/24 brd 10.50.1.255 scope global noprefixroute enp3s0
       valid_lft forever preferred_lft forever
    inet6 fe80::cefd:54d8:f7ef:c892/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

6. Configure the system as a DHCP client
    - Enter `nmtui` at the prompt to open a new interface.

        - Use the `Tab` key and the Arrow keys to navigate text-based user interfaces. Use the `Spacebar` to check/uncheck settings. Use the `Enter` key to accept a configuration.
    - Make sure *Edit a connection* is highlighted, and then press `Enter`.
    - With the interface `<devID>` highlighted from the Ethernet menu, press the Right Arrow key once then the Down Arrow key to highlight < Edit...> and then press Enter.
    - Notice the static IP address, as configured in the previous task.
    - Press the `Tab` key three times to move to the `IPv4 CONFIGURATION line`.
    - That line currently displays `<Manual>`
    - Press `Enter` and select `Automatic` from the menu.
    - Press the `Tab` key multiple times until you reach the bottom of the interface and `< OK >` is highlighted.
    - Press `Enter` to save your changes to the network configuration.
    - Use the `Tab` key to highlight `< Back >` and then press `Enter`.
    - In the `NetworkManager TUI` interface, use the Down Arrow key to highlight `Quit` and then press `Enter`.
    - Enter `ip addr show <devID>` and notice that the old statically assigned IP address is still in place. This is because you need to restart the network service for changes to take effect.
    - Enter `sudo systemctl restart network`
    - Enter `ip addr show <devID>` and notice a new IP address is configured, leased from a DHCP server.
7. Using the GUI, reconfigure the NIC to use a `static IP address`
    - From the desktop menu, select `Applications→System Tools→Settings`.
    - In the `Settings` menu, select `Network`.
    - Notice the wired connection profile is displayed as `Connected` and `On`.
    - Select the `Configuration` gear button.
        - The `NIC` details may still show the `static IP address`.
    - Select the `Apply` button in the upper-right corner of the interface.
    - Select the `slider` to turn the `NIC Off`, then turn it back `On`.
    - Select the `Configuration` gear button again and note the `leased IP address`.
    - Select the `IPv4 tab`.
    - Observe that the Automatic (DHCP) button is selected, as configured in the previous nmtui task.
    - Select the Manual radio button, and then fill in the `Address`, `Netmask`, and `Gateway` fields:
        - `IP address: 10.50.1.101`
        - `Subnet mask: 255.255.255.0 or /24`
        - `Gateway: 10.50.1.1`
    - In the `DNS field`, enter `8.8.8.8`
    - This is one of **Google's DNS servers**.
    - Select `Apply`.
    - Select the slider to turn the connection `Off`, then turn it back `On`.
    - Close the `Settings` window.
    - Test the network configuration by opening `Applications→Favorites→Firefox Web Browser` and browsing to the https://www.comptia.org website.
    - When you're done, close the browser.

Verifying Network Configurations

> Scenario

```
Now that you've configured a NIC, you need to verify that those configurations are
active and accurate. So, you'll use ethtool and the device's configuration file to
confirm the networking details.
```

> Objectives

```
- Completing this activity will help you to use content examples from the
following syllabus objectives:
  - 1.3 Given a scenario, configure and verify network connection parameters
  - 2.7 Explain the use and operation of Linux devices
```

1. Gather information with ethtool
    - If necessary, enter `ip a` to recall your Ethernet device ID.
    - Enter `ethtool <devID>`
    - Verify that you can see information about the NIC's capabilities and configurations.
    - You should be able to see the NIC's maximum bandwidth speed, its duplex capabilities, its supported link modes, and more.
2. View network configuration files
    - Enter `ls /etc/sysconfig/network-scripts` to display the contents.
    - Verify that there is a `ifcfg-<devID>` file.
    - Enter `cat /etc/sysconfig/network-scripts/ifcfg-<devID>` to view the contents.
    - Verify that you can see device information as well as IP addressing information for this NIC.

Configuring a DNS Client

Scenario

```
In addition to setting up machine-friendly IP addressing, you also need to account
for the fact that humans aren't good at remembering long strings of numbers. So,
you'll configure name resolution to relate a hostname with an IP address so that
users can easily refer to a specific computer on the network.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   1.3 Given a scenario, configure and verify network connection parameters
   2.7 Explain the use and operation of Linux devices
```

1. Review the IP address and hostname identities of your system
    - Enter `hostname` to view the system's user-friendly name.
    - Enter `ip addr show <devID>` to view the system's IP address.

        - Humans don't tend to be good at remembering long strings of numbers. Name resolution is used to relate the hostname and the IP address values displayed above.
    - If the leased IP address is still visible, use `nmcli con down <devID>` and then `nmcli con up <devID>` to reset the interface.
2. Try connecting to the second server by name and by IP address
    - Enter `ping server02` and verify that it fails.
    - Enter `ping 10.50.1.102` and verify that it succeeds.
    - Press `Ctrl+C` to interrupt the process.
        - One effective way of testing name resolution is to ping a destination host by name. If that fails, then ping the same host by IP address. If that succeeds, then you know that you have a good network connection to the destination, but that name resolution is failing.
3. Configure the server name for your second server
    - Select `CentOS 7 (2nd)` to access your second virtual machine.
    - Log in as `student02` with `Pa22w0rd` as the password.
    - In a terminal window, enter `sudo hostnamectl set-hostname server02` to configure a new hostname.
    - Enter `sudo systemctl restart systemd-hostnamed` to restart the service, making the change persistent.
    - Verify that your second system's hostname has changed by using the hostname command.
4. Configure name resolution for your system
    - Select `CentOS 7` to return to `server01`. If necessary, use `Pa22w0rd` to sign back in.
    - Enter `cat /etc/resolv.conf` to display the DNS server(s) the system is configured to query.
        - Note the spelling of the file name: `resolv.conf`
    - Enter `cat /etc/hosts` to display the static text file that can be used for name resolution.
    - Using `sudo`, open the text editor of your choice to add your second server's hostname and IP address information into the `/etc/hosts` file in the format: `10.50.1.102 server02`
    - Save and close the file.
    - Ping your second server's hostname and IP address again and verify that, this time, both succeed.
5. Ensure name resolution for Internet identities is functioning correctly
    - Enter `host www.google.com`
    - Enter `nslookup www.google.com`
    - Verify that you receive IP addressing results for google.com with each command.

```
[student01@localhost ~]$ host www.google.com
www.google.com has address 172.217.12.132
www.google.com has IPv6 address 2607:f8b0:4006:801::2004
[student01@localhost ~]$ nslookup www.google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.12.132
```

Configuring Virtualization

Scenario

```
One of the developers at Develetech has asked for your help. She needs Linux test
environments to test that her application functions as designed. She'd like to
manage the environments herself and be able to revert back to their original
configuration for each test. You will install a KVM virtualization solution for
her.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
    1.5 Compare and contrast cloud and virtualization concepts and technologies
```

1. What are some of the potential benefits of virtualization? Click here for answer.

```
Answers will vary. Virtualization can enable easy-to-revert environments;
enable more efficient use of hardware; support on-demand availability;
support quick starting and stopping of environments; offer better support
for disaster recovery; and more.
```

2. Install the KVM virtualization software

   - Enter `cat /proc/cpuinfo | grep vmx` and then enter `cat /proc/cpuinfo | grep svm` to check the processor. If either term is found, the processor should support hardware-assisted virtualization.
   - Carefully enter the following command on one line. Check your syntax before you hit Enter:

```
sudo yum -y install qemu-kvm qemu-img virt-manager libvirt libvirt-python
libvirt-client virt-install virt-viewer bridge-utils librbd1 librbd1-devel
libsolv
```

   - This installs `KVM` and dependent software.
   - Wait for `KVM` to finish installing.
   - Start the `KVM` service
   - Enter `sudo systemctl start libvirtd` to start the service.
   - The name of the KVM service is `libvirtd`
   - Enter `sudo systemctl enable libvirtd` to make the service persist.
   - Enter `lsmod | grep kvm` and verify that the KVM kernel module is loaded.
   - Create a VM at the CLI
   - Carefully enter the following command on one line. Check your syntax before you hit Enter:

```
sudo virt-install --name=devtech-install --vcpus=1 --memory=2048 --
cdrom=/opt/linuxplus/managing_networking/CentOS-7-x86_64-DVD-1810.iso --disk
```

```
size=12 --os-variant=rhel7
```

- This defines the hardware specifications of the virtual machine to create. The VM will use one virtual CPU, have access to 2 GB of RAM, use the provided system image to boot from, and have access to a 12 GB storage drive.
- Close the `devtech-install(1) - VirtViewer` window that pops up and select OK when prompted.
- Enter `sudo virsh save devtech-install saved-vm` to stop the VM and save its state for later.

3. Import a VM image using the GUI Virtual Machine Manager

- From the desktop menu, select `Applications→System Tools→Virtual Machine Manager.`
- Enter the `root` password to continue.
- In the `Virtual Machine Manager`, select `File→New Virtual Machine`.
- In the `New VM wizard`, for the first step, select `Import existing disk image`, then select `Forward`.
- For the second step, select `Browse` and then select `Browse Local`.
- From the navigation menu, select `+ Other Locations`.
- Select `Computer`.
- Navigate to `/opt/linuxplus/managing_networking` and open `ubuntu-vm.qcow2`.
- Select `Forward`.
- For the third step, change the Memory (RAM) to `2048` and ensure CPUs is set at `1`.
- Select `Forward`.
- For the fourth step, name the VM `ubuntu-vm` and select `Finish`.

4. Get acquainted with Ubuntu, a different distribution of Linux

- Verify that a virtual machine window named `ubuntu-vm` on `QEMU/KVM` automatically pops up.
- Wait for the authentication screen (it may take 1-2 minutes).
- Log in to the Ubuntu virtual machine using `student` as the account and `Pa22w0rd` as the password.
- Verify that you successfully signed in to the Ubuntu desktop.
- If you receive an error that there is no space left on the device, reboot CentOS and try again.
- From the bottom-left corner, select the `Show Applications` button  . You might need to scroll the VM window down to locate this button.
- If at any time you're prompted by the `Software Updater dialog box,` select `Remind Me Later`.
- Select the `Settings` icon.
- In the `Settings` window, from the navigation menu, select `Network`.
- Select the `configuration gear icon` for the `Wired` connection to view the `Ubuntu VM's networking information`.
- Select `Cancel` to close the `Wired` window, then close the `Settings` window.
- From the `Show Applications` menu, select the `Utilities` icon.
- Select the `Logs` icon.

- Observe the log files that are displayed (it may take 1-2 minutes), then close the Logs window when you're done.
- From the dock on the left side of the desktop, select the `Ubuntu Software` icon.
- At the top of the window, select the `Installed` tab.
- Scroll down and verify that Vim is installed, then close the window when you're done.
- Shut down the virtual machine
- Close the virtual machine window.
- Right-click the `ubuntu-vm VM` and select `Shut Down→Shut Down`.
- You may need to issue the shut down command twice.
- Wait for the VM's state to change to `Shutoff`.
- Close `Virtual Machine Manager`.

Testing the Network Environment

Scenario

```
You want to use some of the Linux network troubleshooting utilities so that you
can better understand the Develetech network environment. These will help you
diagnose and solve issues related to latency, lack of hostname resolution,
inability to connect to other hosts, and more.
```

Objectives

```
Completing this activity will help you to use content examples from the following
syllabus objectives:
   1.3 Given a scenario, configure and verify network connection parameters
   2.7 Explain the use and operation of Linux devices
```

1. View network services that are currently listening on the hosts in your network.
   - Enter `ip addr` to verify the system has a correct IP address configuration.
   - When troubleshooting, an IP address that begins with `169.254` indicates the client could not lease an IP address from a DHCP server. The `169.254.0.0` IP address range is known as the Automatic Private IP Address (`APIPA`) range.
   - Enter `ss -l | less` to see what TCP ports your system is currently listening on, then press `q` to return to the prompt.
   - Enter `nc localhost 21`
   - You should receive a "`Connection refused`" error, indicating that your system is not listening on `port 21 (FTP)`.
   - Enter `nc server02 22` to verify that the second lab VM is listening on `port 22 (SSH)`.
   - Press `Ctrl+C` to disconnect.
   - You can use a tool like `nc` to identify network services that aren't listening on the local or remote host.
2. Test public name resolution
   - Enter `host www.comptia.org` at the command prompt.
   - Verify that you resolved the public CompTIA hostname to a specific IP address.

- You can use a name resolution tool like host to ensure that you can establish a connection to hosts using human-friendly hostnames.

3. Capture network traffic
   - Enter `sudo tcpdump -i <devID>` where device ID is your Ethernet device name.
   - Verify that the `tcpdump tool` is listening on the device.
   - Right-click the desktop and select `Open Terminal` to open another terminal.
   - In this new terminal, enter `ping server02 -c 4`
   - In the other terminal window, verify that `tcpdump` captured the `ICMP echo traffic.`
   - You can use a network capture tool like `tcpdump` to learn more about the traffic that is transmitted and received over your network.

```
20:45:52.678323 IP server02 > server01: ICMP echo request, id 27664, seq 1, length 64
20:45:52.678377 ARP, Request who-has server02 tell server01, length 28
20:45:52.678590 ARP, Reply server02 is-at c8:60:00:33:c4:a9 (oui Unknown), length 46
20:45:52.678594 IP server01 > server02: ICMP echo reply, id 27664, seq 1, length 64
20:45:53.678387 IP server02 > server01: ICMP echo request, id 27664, seq 2, length 64
20:45:53.678426 IP server01 > server02: ICMP echo reply, id 27664, seq 2, length 64
20:45:54.678387 IP server02 > server01: ICMP echo request, id 27664, seq 3, length 64
20:45:54.678420 IP server01 > server02: ICMP echo reply, id 27664, seq 3, length 64
20:45:55.678380 IP server02 > server01: ICMP echo request, id 27664, seq 4, length 64
20:45:55.678419 IP server01 > server02: ICMP echo reply, id 27664, seq 4, length 64
```

   - Close the terminal window running the tcpdump capture.

11: Managing Packages and Software

Managing Software with RPM and YUM

Scenario

> One of the other `Develetech` administrators has asked you to demonstrate the software management lifecycle on a CentOS server. You will use the `KornShell` (`ksh`) as an example of how to use the `rpm` command, and then the `Very Secure FTP daemon` (`vsftpd`) to demonstrate the `yum` command.

- Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 2.1 Given a scenario, conduct software installations, configurations, updates, and removals

1. Use the `rpm` command to manage the software lifecycle

   - Log in as `student01` with `Pa22w0rd` as the password.
   - Open a terminal.
   - Enter `sudo rpm -ivh /Packages/ksh-20120801-139.el7.x86_64.rpm` to install the `ksh` package in verbose mode and with a hash progress bar.
     - Don't forget to use tab completion for long filenames!
   - Enter `rpm -qi ksh` to view information on the `ksh` package.
     - `ksh` is another shell environment, similar to `bash`. It is common on Unix servers.
   - Enter `sudo rpm -Vv ksh` to verify the `ksh` installation.
   - Enter `sudo rpm -ql ksh` to list the files in the `ksh` package.
   - Enter `sudo rpm -e ksh` to "erase" or uninstall the `ksh` package.

2. Use the `yum` command to manage the software lifecycle

   - Enter `yum` info `vsftpd` to discover information about the `vsftpd` package.
     - `vsftpd` is the Very Secure FTP service.
   - Enter `sudo yum localinstall /Packages/vsftpd-3.0.2-25.el7.x86_64.rpm` to install the `vsftpd` package.
     - You may receive a repeating messages that says an "Existing lock /var/yum/yum.pid: another copy is running." Open a second tab in the terminal (or a second instance of a terminal), and then enter the following command:

```
sudo systemctl kill packagekit
```

   - Enter y when prompted to complete the installation.
     - If you include a `-y` option with `yum`, it will automatically answer yes to this prompt regarding installing dependencies and not pause the installation.
   - Enter `yum info vsftpd` to view information on the `vsftpd` package.

- Enter `yum provides /etc/vsftpd/vsftpd.conf` to discover what package the configuration file belongs to.
- Enter `sudo yum -y remove vsftpd` to uninstall the `vsftpd` package.

Managing Software with dpkg and APT

> Scenario

```
Some Linux systems in Develetech run Ubuntu and other versions of Debian. Just
like your Red Hat-based systems, these need to undergo network troubleshooting
from time-to-time. So, you'll download and install the nmap package on these
machines to ensure you have the right toolset for the job. You'll use dpkg and
APT.
```

Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 2.1 Given a scenario, conduct software installations, configurations, updates, and removals

1. Load the Ubuntu VM
   - From the desktop menu, select `Applications→System Tools→Virtual Machine Manager`.
   - Enter the root password.
   - Right-click `ubuntu-vm` and select `Run`.
   - Right-click `ubuntu-vm` and select `Open`.
   - Wait for the VM to load.
   - Select the student account, then enter `Pa22w0rd` as the password.

     ```
     Recall that there are two primary branches to the Linux family: those
     distributions derived from Red Hat and those derived from Debian. One
     of the key differences between the two branches is software management.
     The Red Hat distributions use rpm and yum, while the Debian
     distributions use dpkg and apt.
     ```

2. Update the `APT database` with current package version information
   - Right-click the desktop and select `Open Terminal`.
   - Enter `sudo apt update`
   - Enter the password when prompted.

     > If the Ubuntu VM has no Internet connectivity, you may need to restart your CentOS host and then reload the VM.

- Verify that the database update operation completed.
- You're presented with the number of packages that can be upgraded. If you wanted to upgrade an existing package, you could use the `apt upgrade {package name}` command. For now, you'll install a new package.

3. Download and install the nmap package

- Enter `sudo apt install nmap`

> If you receive a "Could not get lock..." error, it means the APT package manager is automatically checking for updates. You could wait a few moments or enter the following commands to clear the lock:

- `sudo ps aux | grep apt`
- Observe the process ID number for the process related to `/var/lib/apt/apt.systemd.daily`
- `sudo kill -9 PID` where `PID` refers to the process ID number identified above
- `sudo rm /var/lib/dpkg/lock`
- If necessary, repeat the `sudo apt install nmap command`.
- Enter `y` to confirm the operation.

> You might need to maximize the VM window or scroll to see the prompt asking you to confirm the operation.

- Wait for the installation to complete.
- Enter `apt show nmap` to discover information about the `nmap` package.
- Enter `nmap localhost` to test the utility, confirming that it executes and checks the VM's basic network functionality.

4. Shut down the VM.

- From the `Virtual Machine Manager (VMM)` interface, select `Virtual Machine→Shut Down→Shut Down`.
- Close the VM window.
- Close the `Virtual Machine Manager` window.

Configuring Repositories

> Scenario

```
While the Linux vendors tend to provide online repositories, one of the concerns
with using these is version control of applications. Develetech has decided to
manage an internal repository of software packages, making version control much
easier. You will configure a local `YUM` repository on the CentOS server. You will
then make a `YUM` repository available using `Apache HTTP Server`.
```

Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:

- 2.1 Given a scenario, conduct software installations, configurations, updates, and removals

1. Configure a local `YUM` repository

   - If necessary, open a terminal.
   - Browse to `/Packages` and view the available `.rpm` files.
   - Enter `sudo createrepo /Packages` to designate that directory as a `YUM` repository.
   - This may take a few minutes.
   - Using `sudo`, create a file named `/etc/yum.repos.d/local-repo.repo` with the text editor of your choice.
   - Edit this file by providing the following values:
     - Note that there are three forward slash characters in the `baseurl` path.

```
[local-repo]
name=Local Repository
baseurl=file:///Packages
enabled=1
gpgcheck=0
```

   - Save and close the file.

2. Verify the location is recognized as a YUM repository

   - Enter `yum clean all`
   - Enter `yum repolist` and verify the `local-repo` is displayed.
   - Enter `sudo yum -y --enablerepo=local-repo install ksh` to install the `ksh (KornShell)` package from the repository.

3. Install `Apache HTTP Server` to use as a repository

> You can configure an Apache web server as a repository that provides packages to servers on your internal network.

   - Enter `sudo yum -y install httpd`
   - Enter `sudo systemctl start httpd` to start the Apache service.
   - Enter `systemctl status httpd` and verify that Apache is active (running).

4. Designate Apache as a repository

   - Enter `sudo ln -s /Packages /var/www/html/packages` to link the `/Packages` directory to Apache.
   - Enter `sudo createrepo /var/www/html/packages` to designate the location as a YUM repository.

5. Create the repository reference file

   - Using `sudo`, create a file named `/etc/yum.repos.d/internal-repo.repo` with the text editor of your choice.
   - Edit this file by providing the following values:
     - Note that there are three forward slash characters in the baseurl path.

```
[internal-repo]
name=Internal Repository
baseurl=http://localhost/packages
enabled=1
gpgcheck=0
```

- Save and close the file.

6. Verify the location is recognized as a `YUM` repository
   - Enter `yum clean all`
   - Enter `yum repolist` and verify the `internal-repo` is displayed.
   - Enter `sudo setenforce 0`
   - This disables `SELinux`, an access control mechanism that would otherwise prevent access to the web-hosted packages.
   - Enter `firefox http://localhost/packages` to see a list of packages from the `Apache web server`.
   - Close `Firefox` when you're done.
   - Enter `sudo setenforce 1` to re-enable `SELinux`.
   - Enter `cd ~` to return to your home directory.

Acquiring Software

> Scenario

```
You are investigating ways of downloading software from the web. Specifically, you
are considering writing a script to automate the download process. You will use
wget and curl to try the downloads manually.
```

- Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:

> 2.1 Given a scenario, conduct software installations, configurations, updates, and removals

1. Use the `wget utility` to download a file from the web
   - At a terminal, ensure you're in your home directory.
   - Enter `wget https://download.samba.org/pub/samba/samba-latest.tar.gz` to download the most recent source code file for the Samba service.
   - Check your home directory for a file named `samba-latest.tar.gz`
2. Use curl to download a file from the web
   - Enter `curl -o nmap-7.70.tar.bz2 https://nmap.org/dist/nmap-7.70.tar.bz2` to download version 7.70 of the Nmap utility.
   - Check your home directory for a file named `nmap-7.70.tar.bz2`
3. Expand a source code `tarball` so that it is ready to be compiled in a later activity
   - Enter `tar -xvjf nmap-7.70.tar.bz2` to extract the files.

- Verify that the source code files were extracted in the `~/nmap-7.70/ directory`.
  - You will compile the Nmap utility source files in a later activity. Your current objective is just to acquire and unpackage it.

Compiling and Installing an Application

> Scenario

```
Develetech will be relying on Nmap to troubleshoot its networked systems and
perform vulnerability assessments. You know that compiling Nmap from source code
enables greater flexibility and control. You will do a basic software compile of
Nmap.
```

- Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 2.1 Given a scenario, conduct software installations, configurations, updates, and removals

1. Install the GCC compiler

   - Enter `rpm -qi nmap` to confirm nmap is not already installed.
   - Enter `sudo yum -y install gcc-c++ --disablerepo=internal-repo` to install the necessary GCC compiler for `Nmap`.
   - Wait for the package to finish installing.

2. Compile the Nmap source code

   - Change to the `~/nmap-7.70` directory.
   - Enter `./configure` to generate a makefile based on your system's configuration. This may take a few minutes.
     - Note the `./` characters in the above command. These characters tell bash to "look here" for the executable. By default, bash only checks certain directories for executable commands. Home directories are not usually checked.
   - Enter `make` to compile the software based on the makefile instructions.
   - Enter `sudo make install` to install the binaries on the system.
   - Enter `/usr/local/bin/nmap` and verify that it is installed.
   - The help file for nmap will print to the screen, indicating that the program is installed.
   - Enter `/usr/local/bin/nmap localhost` to scan the local computer.

Securing Linux Systems

Encrypting a Volume

Scenario

```
The data you'll be backing up to your various logical volumes is sensitive in
nature and should not be readable if it were to fall into the wrong hands. To
protect the confidentiality of your backed up data, you'll encrypt the volumes
that hold this data. You'll start with the databk volume. Without the correct key
(e.g., a passphrase), a user will only see the scrambled ciphertext of this
volume, and will be unable to read the plaintext data of individual files.
```

Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: 3.3 Summarize security best practices in a Linux environment

1. Prepare the data backup volume for encryption
    - Log in as `student01` with `Pa22w0rd` as the password.
    - In a terminal window, enter `sudo umount /backup/data`
    - Enter `sudo shred -v --iterations=1 /dev/backup/databk`
    - This will overwrite the contents of the volume to securely wipe any existing data. This is a good practice to ensure that no sensitive data remains before you prepare the encrypted volume.
    - Verify that the `shred` command finishes successfully.
2. Encrypt the data backup volume with a passphrase
    - Enter `sudo cryptsetup -v --verify-passphrase luksFormat /dev/backup/databk`
    - Enter `YES` when prompted to confirm.
    - When prompted for a passphrase, enter `linuxplus`
    - Verify the passphrase.
    - Verify that the command was successful.
3. Open the encrypted volume and verify that it is listed
    - Enter `sudo cryptsetup luksOpen /dev/backup/databk databk`
    - Enter `linuxplus` as the passphrase.
    - Verify that you are returned to a prompt without errors.
    - Enter `ls -l /dev/mapper | grep databk`
    - Verify that the encrypted volume is listed.
4. Format the volume, mount it, and create a file
    - Enter `sudo mkfs.ext4 /dev/mapper/databk`
    - Verify that the file system was written.

- Enter `sudo mount /dev/mapper/databk /backup/data`
- Enter `echo "Encrypted" | sudo tee /backup/data/encrypt.txt`

5. Add the encrypted volume to the `/etc/crypttab` and `/etc/fstab` files

- Enter `sudo bash -c "echo databk /dev/backup/databk none >> /etc/crypttab"`
- Enter `sudo cat /etc/crypttab` and confirm that the line was added.
- `[student01@server01 nmap-7.70]$ sudo cat /etc/crypttab databk /dev/backup/databk none`
- This file is similar to `/etc/fstab` and initializes encrypted storage devices at boot.
- Using `sudo`, open the `/etc/fstab` file in your text editor of choice.
- Edit the line that mounts the `/dev/backup/databk` volume to say the following:
- `/dev/mapper/databk /backup/data ext4 nofail 0 0`
- This will mount the encrypted volume after it has been unlocked. The `nofail` option indicates that the system should not report any errors if the volume is not detected.
- Save and close the file.

6. Reboot the machine and unlock the encrypted volume

- Enter `systemctl reboot -i`
- Verify that, rather than the normal sign in screen, you are prompted to unlock the encrypted volume with your passphrase.
- Enter `linuxplus`
- Sign in as your student account.
- Using your preferred method, open the `/backup/data/encrypt.txt` file and verify you can read its plaintext contents.
- Enter `sudo bash -c "echo > /etc/crypttab"`
- You're clearing this file so you won't be prompted to unlock the volume every time you reboot. You can still unlock the volume manually after you've booted into the OS.
- Encrypting a volume in this way requires physical access to the computer in order to unlock it and complete the boot process. You won't be able to SSH into the system to unlock it.

Configuring SSH Authentication Using a Key Pair

> Scenario

```
You want to enable your fellow administrators to remotely access servers that are
physically located elsewhere. By default, the servers are already set up to accept
encrypted SSH connections. Recently, however, Develetech has been the victim of
several brute force password cracking attempts. Attackers have tried to gain
remote access by running through various combinations of passwords. To minimize
the risk of these attacks, you decide to change the authentication method that
administrators will use to connect remotely. You'll have them each generate a
cryptographic key pair that they'll use to prove their identities. Anyone without
the key will be denied access. You'll also disable password authentication on the
servers to mitigate brute force attacks.
```

> Objectives

> Completing this activity will help you to use content examples from the following syllabus objectives:
> 2.5 Summarize and explain server roles
> 3.2 Given a scenario, configure and implement appropriate access and authentication methods
> 3.3 Summarize security best practices in a Linux environment

1. Generate a public and private key pair to use with SSH authentication

    - Enter `ssh-keygen` to generate a key pair.
    - Press `Enter` to accept the default path in which to save the key.
    - Enter `linuxplus` as the `passphrase`.
    - You don't need to protect a private key with a `passphrase`, but doing so adds a second factor to the authentication process, and is recommended. The `passphrase` will decrypt the private key before it is used to solve the server's encrypted challenge.
    - Enter the `passphrase` again.

2. Verify that the keys were generated and saved to the home directory

    - Enter `cat .ssh/id_rsa` and examine the (encrypted) private key.
    - This is the key you'll use to validate the SSH server's encrypted challenge.
    - Enter `cat .ssh/id_rsa.pub` and examine the public key.
    - The server needs to install this public key once. The server will use this public key to verify the authenticity of the private key.

3. Copy your public key to your second server

    - Enter `ssh-copy-id student02@server02` to copy your public key to `server02`.
    - Enter `yes` to accept the authenticity of your second server.
    - When prompted for a password, enter `Pa22w0rd`

4. Verify that your public key was added to your second server

    - Select CentOS 7 (2nd) and log in as `student02`.
    - Enter `cat .ssh/authorized_keys` and verify that your key was added.
    - Any public keys added to this file are considered authorized and will be used in SSH authentication. If you wanted to authenticate other users, you could have them generate a unique key pair and then add their public key to this file as well.

5. Authenticate with your second server's SSH server using your private key

    - Select `CentOS 7` to return to `server01`.
    - Enter `ssh student02@server02`
    - When prompted, type *(but don't press Enter)* `linuxplus` as the passphrase to unlock your private key.
    - Check the `Automatically unlock this key whenever I'm logged in` check box.
    - Select `Unlock`.
    - Verify that you are signed in to `server02` as the `student02` account.
    - If you get an `"Authentication failed"` message, enter the `ssh` command again.

- You've successfully authenticated to the *second SSH server*.

6. For added security, disable password authentication

   - Enter `exit` to close your SSH session and return to your local login on `server01`.
   - Switch back to the `CentOS 7 (2nd) virtual machine`.
   - Using `sudo`, open the `/etc/ssh/sshd_config` file in your desired text editor.
   - Scroll down until you get to the `PasswordAuthentication yes` line.
   - Change `yes` to `no` and then `save and quit` the file.
   - Enter `sudo systemctl restart sshd`
   - Switch back to `CentOS 7`
   - Enter `ssh ariley@server02`
   - You have no private key for this account, and the server isn't accepting passwords.

Configuring SELinux

> Scenario

```
The Apache web server you installed is serving its purpose, but the team would
like to organize the server's files in a more descriptive way than the default
`/var/www/html` directory. Also, the system will eventually run multiple web apps,
each in a different path. For now, you need to place all of the web server files
in a new `/var/develweb` directory. Even though you apply the correct standard
permissions and configure Apache to allow access, `SELinux` will prevent the
`httpd service` from reading files in this new directory. So, you'll
configure`SELinux` as needed to make sure the web server is operational
```

Objectives

> Completing this activity will help you to use content examples from the following syllabus objectives:
> 3.1 Given a scenario, apply or acquire the appropriate users and/or group permissions and ownership
> 4.3 Given a scenario, analyze and troubleshoot user issues
> 4.4 Given a scenario, analyze and troubleshoot application and hardware issues

1. Check the status of `SELinux`

   - Enter sestatus to display the current status of `SELinux`.
   - Verify that `SELinux` is enabled and in enforcing mode.

2. Create a new directory to hold the web server files

   - Enter `sudo mkdir /var/develweb`
   - Enter `sudo bash -c "echo This is a test > /var/develweb/test.html"`
   - Enter `ls -al /var/develweb`
   - Verify that all users have read and execute permissions to this directory, and that all users have at least read permissions to the file you just created.

3. Configure Apache settings to use the new path as the document root and enable access

- Using `sudo`, open the `/etc/httpd/conf/httpd.conf` in the text editor of your choice.
- Enter `/DocumentRoot` to search for the appropriate field.
- Change this field to the following:
- `DocumentRoot "/var/develweb"`
- Below this, look for the `< Directory "/var/www">` line and change it to the following:
- `< Directory "/var/develweb">`
- There is not a space between `<` and `D`
- Save and quit the file.
- Enter `sudo systemctl restart httpd`

4. Attempt to view the web page, and troubleshoot any issues

- From the desktop menu, select `Applications→Favorites→Firefox Web Browser`.
- Navigate to http://127.0.0.1/test.html
- Verify that you are presented with a `Forbidden message`.
- The message elaborates by saying you don't have permission to access the HTML file.
- An `SELinux alert` will also pop up on the desktop, but will be minimized after a few seconds. The alert may be accessed by selecting the icon that appears to the left of the clock in the taskbar.
- If the `SELinux alert` is still open, hover over it and select `Show`. If the alert disappears, select the icon to the left of the clock to open the same `SELinux Alert Browser dialog box`.
- Select `Troubleshoot.`
- Under `If you were trying to`, select the first option.
- Verify that the proposed solution involves changing the context label on the new directory path.
- The troubleshooter mentions many possible file types, but there is a way to narrow down which one you need to use.
- Close this dialog box.

5. Verify the required SELinux context and the current one applied to the new path

- At a terminal, enter `ls -Z /var/www`
- Retrieving `SELinux` context information from the default document root should provide you with what you need.
- Verify that the "type" context for the html directory is `httpd_sys_content_t`
- This is the context you need to apply to your new directory to allow Apache to access the files.
- Enter `ls -aZ /var/develweb` and verify that the "type" context for your new directory is `var_t`
- This new directory inherited the default context of its container directory `(/var)`.

6. Apply the appropriate context to the new web server directory

- Enter `sudo semanage fcontext -a -t httpd_sys_content_t "/var/develweb(/.\*)?"`
- This adds the provided context for the `/var/develweb` directory. The symbols at the end use a regular expression to apply this context to all subdirectories and files within this directory.
- Enter `ls -aZ /var/develweb` and verify that the directory still doesn't have the correct context.
- Enter `sudo restorecon -Rv /var/develweb`
- Check the directory's contexts again and verify that it now shows `httpd_sys_content_t`

7. Confirm that you can now access the web page.

- Switch back to `Firefox` and refresh the page.
- Verify that the test page is displayed.
- Close the browser.

Configuring a Firewall

> Scenario

Your fellow network administrators have designed a `DMZ` in which you'll need to place several public-facing Linux systems. For the most part, these systems function as web servers, and need to allow users to connect using the `HTTP` and `HTTPS` protocols. The servers are also running a custom app that the development team has programmed to accept connections on `port 7743`. So, your job is to tighten the network security of the servers without denying access to the necessary services. You'll do this by configuring the `firewalld` service, the default and preferred firewall service on `CentOS 7`

> Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 3.5 Given a scenario, implement and configure Linux firewalls
  - 4.4 Given a scenario, analyze and troubleshoot application and hardware issues

1. Test the firewall to see if it's blocking a well-known port

   - Switch to `CentOS 7 (2nd)`
   - Enter `systemctl status firewalld`
   - Confirm that the service is currently active and running.
   - If it isn't, enter `sudo systemctl start firewalld`
   - Switch to `CentOS 7`
   - Enter `sudo /usr/local/bin/nmap -sV server02 -p 80`
   - Verify that `port 80/tcp` is listed as "filtered", meaning that a firewall is likely blocking traffic on this port.

2. Get more information about a specific zone

   - Switch to `CentOS 7 (2nd)`
   - Enter `firewall-cmd --get-zones` to get a list of all default zones.
   - Enter `sudo firewall-cmd --zone=dmz --list-all`
   - Verify that you see several details about this zone, including:
   - Its target. The target defines the behavior for incoming connections (i.e., accept, reject, or drop traffic). The default setting is to reject traffic not matching any rules.
   - What network interfaces this zone is currently applied to.
   - What services, ports, and protocols are applied to this zone. In this case, SSH is the only service that will accept incoming connections on interfaces that use this zone.
   - Additional rules for *port forwarding*, *blocking ICMP (ping)*, and more.
   - Enter `sudo firewall-cmd --get-active-zones`
   - Verify that, currently, your main Ethernet interface is using the public zone.

3. Set the `dmz zone` for your primary network interface

- Enter `ip a` and note the device name of your primary Ethernet interface.
- This is the interface that you configured in the networking lesson.
- Enter `sudo firewall-cmd --zone=dmz --change-interface=ens32 --permanent`
- Verify that the change was a success.

4. Add services and a custom port to the zone

- Enter `sudo firewall-cmd --zone=dmz --add-service=http --permanent`
- Enter `sudo firewall-cmd --zone=dmz --add-service=https --permanent`
- You've just added `HTTP` and `HTTPS` as services that will apply to the dmz zone. In other words, traffic bound for these services will be allowed.
- Enter `sudo firewall-cmd --zone=dmz --add-port=7743/tcp --permanent`
- This adds a specific port instead of a defined service to the zone.

5. Verify that your configurations were applied to the zone

- Enter `sudo firewall-cmd --reload`
- Enter `sudo firewall-cmd --zone=dmz --list-all`
- Verify the following about this zone:
- It is being used by your main network interface.
- The `SSH`, `HTTP`, and `HTTPS` services are active in the zone.
- `TCP port 7743` is also active in the zone.

6. Test the firewall to see if your configurations are working as intended

- Switch to `CentOS 7`
- Enter `sudo /usr/local/bin/nmap -sV server02 -p 80`
- Verify that the port is now "*closed*," indicating that the firewall permits traffic on this port, but there is not a service currently listening on this port.
- Use the same `nmap` command to scan for `port 21 (FTP)`.
- Verify that it is filtered, indicating that the firewall is blocking traffic on this port as expected.
- Enter `ssh student02@server02`
- Verify that you are able to make a connection, indicating that SSH traffic is allowed.
- Enter `exit` to close the SSH session.
- What is the Linux kernel framework that most firewall services rely on to some degree? Click here for the answer.
  - > Netfilter
- In an iptables table, what is the function of a chain, and how do chains interact with one another? Click here for the answer.
  - > Chains are sets of rules that the table uses to implement firewall functionality. Chains enable a progression of how firewall rules are evaluated; traffic matching a

> rule in one chain can be passed to another chain, where it is evaluated against a new set of rules.

- True or false? `IP forwarding` is most useful on systems with only one network interface. Click here for the answer.
  - > False
- What are the differences between a firewall and an `intrusion prevention system (IPS)`? Click here for the answer.
  - > Answers may vary, but firewalls typically allow or deny traffic into and out of a network based on a set of predefined rules. An IPS evaluates traffic that has made it past the firewall and looks for a repeated pattern of anomalous or otherwise unwanted behavior. An IPS is therefore a second layer of defense. Firewalls can also apply to outgoing traffic, whereas IPSs tend to focus on just incoming traffic.

Configuring rsyslog for Local and Remote Logging

> Scenario

```
You want to ensure that your system is logging only messages that are useful to
you and other analysts. So, you'll configure the local logging behavior to be more
fine-tuned and less noisy. In addition, each system should be sending its
authentication logs to a remote, centralized server for easy analysis and storage.
So, you'll configure rsyslog to send these messages to a remote host over the
network
```

> Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 2.5 Summarize and explain server roles
  - 3.4 Given a scenario, implement logging services

1. Examine the default rules in the rsyslog configuration
   - On CentOS 7 using `sudo`, open the `/etc/rsyslog.conf` file in the text editor of your choice.
   - Scroll down to the `RULES section`.
   - Verify that, in the left column, each line lists one or more severities and/or facilities.
   - For example, the `authpriv._facility` refers to private authentication messages, such as login and logout events. The `asterisk (*)` indicates that all severities should be logged.
   - Verify that each line has a corresponding action in the right column.
   - For example, the `authpriv.*` facility will log its messages in the `/var/log/secure` file.
2. Filter the messages log to reduce the number of events it records
   - Locate the line that logs events to the `/var/log/messages file`. This line tells `rsyslogd` to log all events that are of `info level (6)` severity and above *(lower number is more severe)*. It

makes exceptions for `mail messages`, `private authentication messages`, and `cron` messages (scheduler).
- On this line, replace the `.info` text with `.notice`
- The notice `severity (level 5)` logs normal but significant conditions. Now, the messages log will not record `informational messages (level 6)`, but start with `level 5` messages.
- Leave the file open.

3. Configure your `server02` to receive `remote rsyslog messages over TCP`

- On `CentOS 7 (2nd)` use `sudo` to open `/etc/rsyslog.conf` in the text editor of your choice.
- Scroll to the `MODULES` section.
- Find the line that says `# Provides TCP syslog reception`
- Change the two lines below so that they read as follows:
- `$ModLoad imtcp`
- `$InputTCPServerRun 601`
- Ensure there are no `#` symbols at the beginning of these lines.
- Save your changes and close the file.
- Enter `sudo systemctl restart rsyslog` to restart the service, causing it to reread the configuration file and implement your changes.

4. Configure the client to send `rsyslog` traffic to `server02`

- Switch to the `CentOS 7 virtual machine`.
- Scroll to the bottom of the `/etc/rsyslog.conf` file, and on a new line, type the following:
- `authpriv.\* @@10.50.1.102:601`
- Ensure there are no leading `#` symbols on this line.
- The `@@` symbols indicate a `TCP` connection, whereas a single `@` indicates `UDP`.
- Save and close the file.
- Enter `sudo systemctl restart rsyslog` to restart the service, causing it to reread the configuration file and implement your changes.

5. Add an allow rule to the firewall for the `rsyslog` traffic

- Switch to the `CentOS 7 (2nd) virtual machine`.
- Enter `sudo firewall-cmd --zone=dmz --add-port=601/tcp --permanent`
- Enter `sudo systemctl restart firewalld`

6. Generate an authentication failure message and confirm it was sent to your second server

- Switch to the `CentOS 7 virtual machine`.
- Enter `su - ariley`
- Provide an incorrect password and verify that you failed to log in as this user. By entering the wrong password, you will generate a log file entry.
- Switch to `CentOS 7 (2nd)`
- Enter `sudo tail /var/log/secure | grep ariley`
- Verify that you see an authentication failure message that was sent from your other server.

7. Turn off remote logging

- Switch to `CentOS 7`

- Using `sudo`, open the `/etc/rsyslog.conf` file in the text editor of your choice.
- Scroll to the **bottom of the file** and remove the entire `authpriv line`.
- Save and close the file.

Examining Log Files

> Scenario

```
Up until now, you've examined a few logs using standard tools like cat and less,
and also filtered those logs using a tool like grep. However, you can also use
`journalctl` to more efficiently shape those log messages in order to extract the
specific information you're looking for. You'll also use last and its associated
commands to get an overview of login events, such as when a user last logged in
```

> Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 2.5 Summarize and explain server roles
  - 3.4 Given a scenario, implement logging services

1. Use `journalctl` to retrieve and filter messages
   - Enter `sudo journalctl` and verify that you can page through many lines.
   - Press `q` to quit.
   - Enter `sudo journalctl -p` notice and verify that the log was filtered.
   - Only messages matching *severity level 5* appear.
   - Press `q` to quit.
   - Enter `sudo journalctl -p notice | grep kernel`
   - Verify that kernel messages are displayed.
   - These messages are similar to what you'd find in the `/var/log/messages` file.
   - Enter `sudo journalctl -f` to retrieve the most recent entries.
   - Press Ctrl+C to terminate the process.
   - Enter `sudo journalctl --since "2 hours ago" --until "30 minutes ago"`
   - Page through the results and verify that the first entry was two hours ago and that the last entry was 30 minutes ago.
   - Press `q` to quit.
   - Enter `sudo journalctl -u httpd.service`
   - Verify that the log is filtered by ***Apache service messages***.
   - Press `q` to quit.

2. Use `last` and related commands to examine account login events Enter `last` Verify that you can see the login and logout events for various users. Enter `sudo lastb` Verify that you can see a list of user accounts and the times that an authentication attempt with that account failed. Enter `lastlog` Verify that you can see the last time that each user logged in. This log also indicates when an account has never logged in.

Archiving and Restoring Files

> Scenario

```
On a yearly basis, HR has been compiling information about Develetech employees
and putting them in a spreadsheet. These spreadsheets contain personal information
such as names, addresses, and phone numbers. You need to ensure that past years'
reports are stored in backup should they ever need to be retrieved in the future.
Because you won't need to regularly update these files, you decide to place them
in a single archive. You also want to test the process of recovering the files
from this archive if it's ever necessary
```

> Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: 3.6 Given a scenario, backup, restore, and compress files

> If necessary, unlock the encrypted volume. Open the Files app, then select + Other Locations, then select the encrypted volume and input linuxplus as the passphrase.

1. Copy the employee data files to your home directory
    - Ensure you are in your home directory.
    - Enter `cp -r /opt/linuxplus/securing_linux_systems/employee_data employee_data`
    - Enter `ls -l` and verify that the directory was copied.
2. Archive the employee data files and then copy the archive to the data backup volume
    - Enter `tar -cvf employee_data.tar employee_data/_`
    - This creates a new archive with the specified name. The `asterisk (*)` indicates that all files within the employee_data directory should be added to the archive.
    - Enter `ls -l` and verify that the `.tar` file is present.
    - Enter `tar -tf employee_data.tar` to list the contents of the archive.
    - Enter `sudo cp employee_data.tar /backup/data/employee_data.tar`
    - Enter `ls -l /backup/data` and verify that the archive file is now on the data backup volume.
3. Restore all files from the archive, then restore a single file.
    - Enter `cd /backup/data` to change your current working directory.
    - Enter `sudo tar -xf /backup/data/employee_data.tar`
    - Enter `ls -l employee_data` and verify that all of the files were extracted to the directory.
    - Enter `sudo rm -r employee_data` to delete the directory.
    - Enter `sudo tar -xf employee_data.tar employee_data/emp_2018.csv`
    - Enter `ls -l employee_data` and verify that only the one file was extracted.
    - Enter sudo rm -r employee_data to delete the directory.

Synchronizing Files

Scenario

```
The Research and Development (R&D) department also has sensitive data that they
need backed up: data on product prototypes, including model numbers, pricing, and
release dates. Unlike the employee data, these files are likely to be updated
regularly. So, you want to make sure the backup copies consistently align with the
source copies. You'll use rsync to synchronize both copies, ensuring that the
backup copies will only need to be updated if the source files have changed
```

> Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: 2.3 Given a scenario, create, modify, and redirect files 3.6 Given a scenario, backup, restore, and compress files

1. Copy the prototype product files to your home directory
    - Enter `cd ~` to return to your home directory.
    - Enter `cp -r /opt/linuxplus/securing_linux_systems/prototypes prototypes`
    - Enter `ls -l` and verify that the directory was copied.
2. Synchronize the prototype files with a directory on the backup volume
    - Enter `sudo rsync -av prototypes /backup/data`
    - In the output, verify that each file in the folder was copied, and that the command sent a specific number of bytes.
    - Enter `ls -l /backup/data` and verify that all files were copied.
3. Make a change to a file and resynchronize with the backup directory
    - Enter `echo -e "\nSW950,749.99,12/5" >> prototypes/swatch.csv` to make a change to one of the files.
    - Enter `sudo rsync -av prototypes /backup/data`
    - In the output, verify that the only file that was sent was the one that you changed.

```
[student01@server01 ~]$ sudo rsync -av prototypes /backup/data
sending incremental file list
prototypes/swatch.csv

sent 377 bytes  received 36 bytes  826.00 bytes/sec
total size is 667  speedup is 1.62
```

    - Enter `cat /backup/data/prototypes/swatch.csv` and verify that your change was added to the backup version of the file.

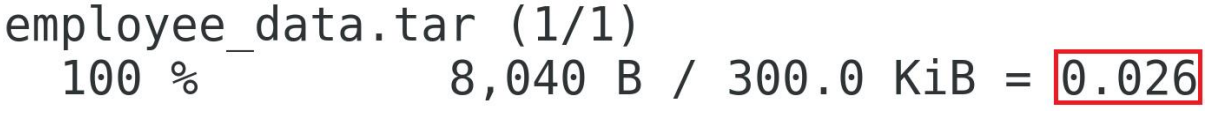
Compressing Files

> Scenario

As you archive more and more data, you realize that the archives take up just as much space as the files they hold. This is a waste of space, especially if you're not working with the archives' contents regularly. So, you'll compress the archives so that they take up significantly less space without losing any data. You'll also try several different compression algorithms and compare their performance

> Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 2.3 Given a scenario, create, modify, and redirect files
  - 3.6 Given a scenario, backup, restore, and compress files

1. Note the size of the employee data archive on the backup volume
   - Enter `cd /backup/data`
   - Enter `ls -lh` and note the size of the `employee_data.tar` file that you created earlier.
2. Compress the archive with `gzip`
   - Enter `sudo bash -c "gzip -cv employee_data.tar > employee_data.tar.gz"`
   - Verify that the output indicates that the file was reduced by over 90% of its original size.
   - By default, `gzip` replaces the file with the compressed version. With this command, you are using the `-c` option with output redirection to keep the original .tar file intact. Enter `ls -lh` and confirm that `employee_data.tar.gz` is much smaller in size.
3. Decompress the archive
   - Enter `sudo tar -xzf employee_data.tar.gz`
   - Enter `ls -l employee_data` and verify that the individual files were extracted.
   - With the `-z` option, the tar command has the ability to use `gzip` to compress and decompress archives. You could use `gzip` to decompress the file and then `tar` to unarchive it, but this is faster.
   - Enter `sudo rm -r employee_data` to delete the directory.
4. Compress and decompress the archive with `xz`
   - Enter `sudo xz -kv employee_data.tar`
   - The `-k` option keeps the original file intact.
   - Verify that the output indicates that the compressed file is less than 5% the size of the original (expressed in decimal).
   - 

   - Enter `ls -lh` and verify that the `employee_data.tar.xz` file is even smaller than the `.gz` file.
   - Enter `sudo tar -xJf employee_data.tar.xz`
   - The `tar` command can also work with `.xz` files through the `-J` option. As before, this decompresses and unarchives the `.tar` archive all in one command.
   - Enter `ls -l employee_data` and verify that all of the files are there.
   - Enter `sudo rm -r employee_data` to delete the directory.
5. Compress and decompress the archive with bzip2
   - Enter `sudo bzip2 -kv employee_data.tar`
   - Verify that the output indicates that the file was reduced by over 90% of its original size.
   - Enter `ls -lh` and confirm that `employee_data.tar.bz2` is slightly larger than the `.gz` equivalent.
   - Enter `sudo tar -xjf employee_data.tar.bz2`

- The `tar` command can also work with `.bz2` files through the `-j` option. As before, this decompresses and unarchives the `.tar` archive all in one command.
- Enter `ls -l employee_data` and verify that all of the files are there.
- Enter `sudo rm -r employee_data` to **delete** the directory.

Performing Integrity Checks on Files

> Scenario

The R&D team is concerned about unauthorized users tampering with the prototype data. There's also the possibility that the data will become corrupted in a non-obvious way, which will compromise the integrity of the data. So, in order to be confident that the data hasn't changed, you'll run the files through a hash function and compare those hashes to hashes captured at a different time. If the hash values are the same, you can be assured of the data's integrity. If not, you'll know something went wrong

> Objectives

Completing this activity will help you to use content examples from the following syllabus objectives: 3.6 Given a scenario, backup, restore, and compress files

1. Create hashes of the prototype files

   - Enter `sudo bash -c "sha256sum prototypes/\* > hashes.txt"`
   - Enter `sudo cat hashes.txt`
   - Verify that the text file lists five different hash values, each one corresponding to a specific `.csv` file.

```
61266b2d7504071517f155db57e0d5c8808c6dde88180993f29d52b6fcb4e928  prototypes/gpu.csv
a49ed2f1b22bab6c02e7bd179a3b71a7be9ffcb2649dbc47960956e521554436  prototypes/hmd.csv
d38a12ace1a535f3e68635d6a4996590ecf20e51845a22239320167d8d1dae42  prototypes/ssd.csv
9c4b601e56b08b09a8979b1e373143c738d19ff091f55ff3fbb2209cc9827a1f  prototypes/stv.csv
f0874265115269d2c8b69d2a9ad2ed7f064efc496efe508e246d6b804bfa9289  prototypes/swatch.csv
```

2. Compare the captured hashes to the hashes of the current files

   - Enter `sudo sha256sum -c hashes.txt`
   - Verify that the output indicates that all of the files are "`OK`".
   - In other words, `sha256sum` hashed the files, then compared those hashes to the list of hashes you generated in the previous step. The hashes are all identical, implying that the files haven't changed. In a production environment, you'd compare these hashes after some time had passed, after some potentially disruptive event, or right before resynchronizing.

3. Make changes to the files and verify that they fail the integrity check

   - Enter `sudo bash -c "echo GPU999 >> prototypes/gpu.csv"`
   - Enter `sudo rm prototypes/hmd.csv`
   - Enter `sudo sha256sum -c hashes.txt`
   - Verify that, this time, the integrity check failed on the file you modified, and that it could not find the file you deleted.

```
prototypes/gpu.csv: FAILED
sha256sum: prototypes/hmd.csv: No such file or directory
prototypes/hmd.csv: FAILED open or read
prototypes/ssd.csv: OK
prototypes/stv.csv: OK
prototypes/swatch.csv: OK
sha256sum: WARNING: 1 listed file could not be read
sha256sum: WARNING: 1 computed checksum did NOT match
```

13: Working with Bash Scripts

Customizing the Bash Shell Environment

Scenario

In order to enhance your productivity at the CLI, you decide to customize your Bash shell environment. For security reasons, you want to minimize the number of commands that are kept in the shell history, so you'll adjust the appropriate environment variable. You also plan on creating a directory to hold your future scripts, and in order to easily execute the scripts in that directory, you'll need to add it to your search paths. Lastly, as part of your auditing duties, you find yourself entering a rather lengthy command at the CLI every so often; this can get tedious, so you'll create a short alias for that command to make things easier.

> Objectives Completing this activity will help you to use content examples from the following syllabus objectives: 5.1 Given a scenario, deploy and execute basic Bash scripts

1. Display the current environment variables
    - Log in as `student01` with `Pa22w0rd` as the password.
    - Open a terminal window.
    - Enter `env` to display environment variables.
    - Verify that the current environment variables and their values appear on the screen.
    - Verify that the `HISTSIZE` variable has a value of `1000`, indicating that a maximum of 1,000 of the most recently entered commands are stored in memory.
2. Reduce the maximum size of the command history by exporting its environment variable
    - Enter `echo $HISTSIZE` and verify that the variable has the expected value.
    - Enter `export HISTSIZE=5`
        - This is value is intentionally low to make it easier to demonstrate.
    - Enter more than five unique commands, one after another.
    - For example, you could enter `echo 1`, `echo 2`, etc.
    - Press the Up Arrow and verify that you can only return, at most, to the fifth-most recent command.
        - You can revert the history size if you prefer, or you can log out and it will revert automatically.
3. Create a directory that will hold scripts
    - Enter `sudo mkdir /scripts`
    - Enter `sudo cp /opt/linuxplus/working_with_bash_scripts/testscript.sh /scripts/testscript.sh`
    - Enter `testscript.sh`
    - Verify that the command was not found.
        - Bash is configured to check only certain directories for executable files, and because the `/scripts` directory is not one of the places it checks, it does not find your script.
4. Add `/scripts` as a search path to persist for the student account

- Enter `echo $PATH` to display the directories that `Bash` does check for executable files.
- Verify the current search paths that are set in this environment variable.
- Ensure you are in your home directory. Enter `cd ~` to move to your home directory.
- Open `.bash_profile` in the **text editor** of your choice.
- Scroll to the last line of the file and change it to the following:
- `export PATH=$PATH:/scripts`
  - Ensure you are appending /scripts to the`$PATH`variable, or you will overwrite the existing paths and be unable to easily enter many commands.
- Save and close the file.

5. Test that the path works as intended

- Enter `source .bash_profile` to reload your Bash profile and its variables.
- Open a terminal and enter `echo $PATH` and verify that the new path was added to the end of the variable.
  ```
  [student01@server01 ~]$ echo $PATH
  /usr/lib64/qt-3.3/bin:/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/
  bin:/sbin:/home/student01/.local/bin:/home/student01/bin:/home/student01/
  .local/bin:/home/student01/bin:/scripts
  ```
- Enter `testscript.sh` and verify that the script executed successfully.

6. Create an alias for a lengthy command

- Enter `lastlog | tail -n +2 | sort -k1`
- Verify that the list is sorted by user name, rather than the default of last login time.
- This is a somewhat cumbersome command to type over and over, so you'll create an alias to save time.
- Open `.bashrc` in the text editor of your choice.
- At the bottom of the file, on a new line, type the following:
- `alias ulog='lastlog | tail -n +2 | sort -k1'`
- Save and close the file.
- Enter `source .bashrc`
- Enter `ulog` and verify that it produced the expected results.

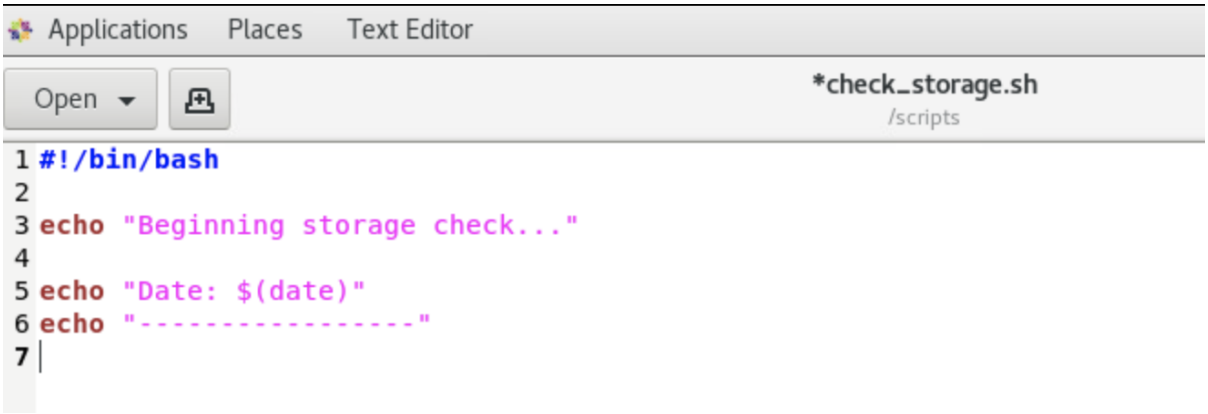
Writing and Executing a Simple Bash Script

> Scenario

```
As part of managing the many storage partitions and volumes on your Linux servers,
you routinely run a command like df to see if any devices are getting close to
full. By monitoring the storage space being used by each device, you can avoid
problems before they happen. However, entering this command over and over again is
somewhat tedious, and it doesn't immediately retrieve the most relevant
information in the most useful format. You want to be able to generate a more
readable "dashboard" report of what storage devices are getting close to full, and
which are fine. So, you decide to automate the process by writing a script to do
the work for you.
```

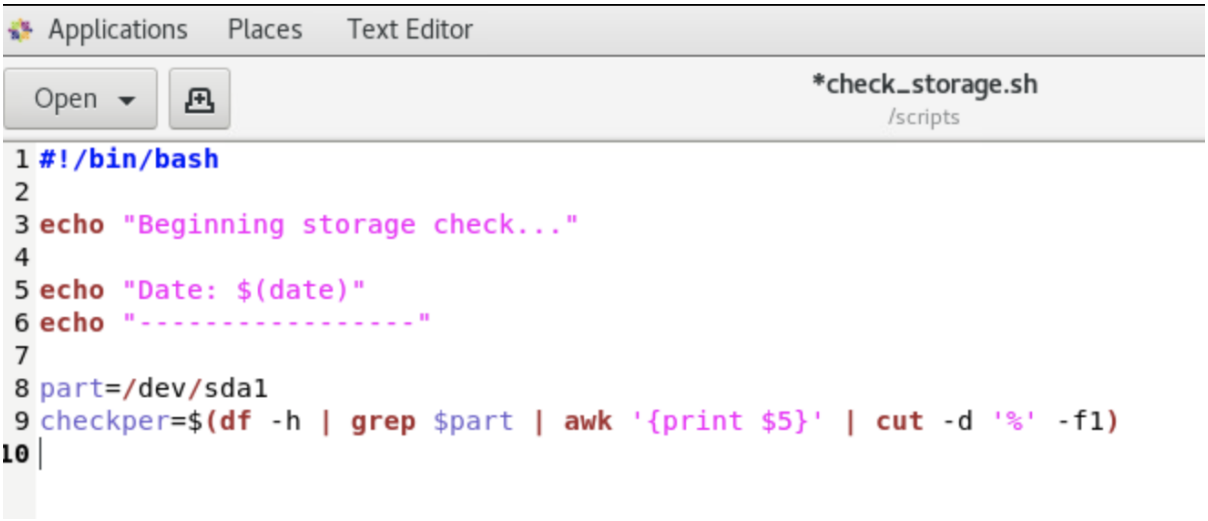
> Objectives Completing this activity will help you to use content examples from the following syllabus objectives: 5.1 Given a scenario, deploy and execute basic Bash scripts

1. Create the script file and give yourself the necessary permissions to execute it
    - Enter `sudo touch /scripts/check_storage.sh`
    - Enter `sudo chown student01 /scripts/check_storage.sh`
    - Enter `chmod 755 /scripts/check_storage.sh`
    - You're giving yourself full access and everyone else read and execute permissions.
2. Set up your script editing environment
    - From the desktop menu, select `Applications→Accessories→Text Editor`.
    - > You can write source code at the CLI, but it's often easier to write it in a visual editor, especially if you're new to programming/script writing.
    - Select `Open→Other Documents`.
    - Navigate to `/scripts` and open `check_storage.sh`.
    - On the bottom-right of the window, select the `Ln 1, Col 1` drop-down list.
    - Check the Display line numbers check box.
3. Begin the script by writing some contextual echo statements
    - On line 1, type `#!/bin/bash`
    - Press Enter twice to skip to line 3.
    - Type `echo "Beginning storage check…"`
    - On new lines 5 and 6, type the following:
    - `echo "Date: $(date)"`
    - `echo "-----------------"`
    - The first line will simply echo the current date and time. It does this by leveraging the date command using command substitution. The second line just makes the formatting a little more visually pleasing; you don't need type an exact number of hyphens.



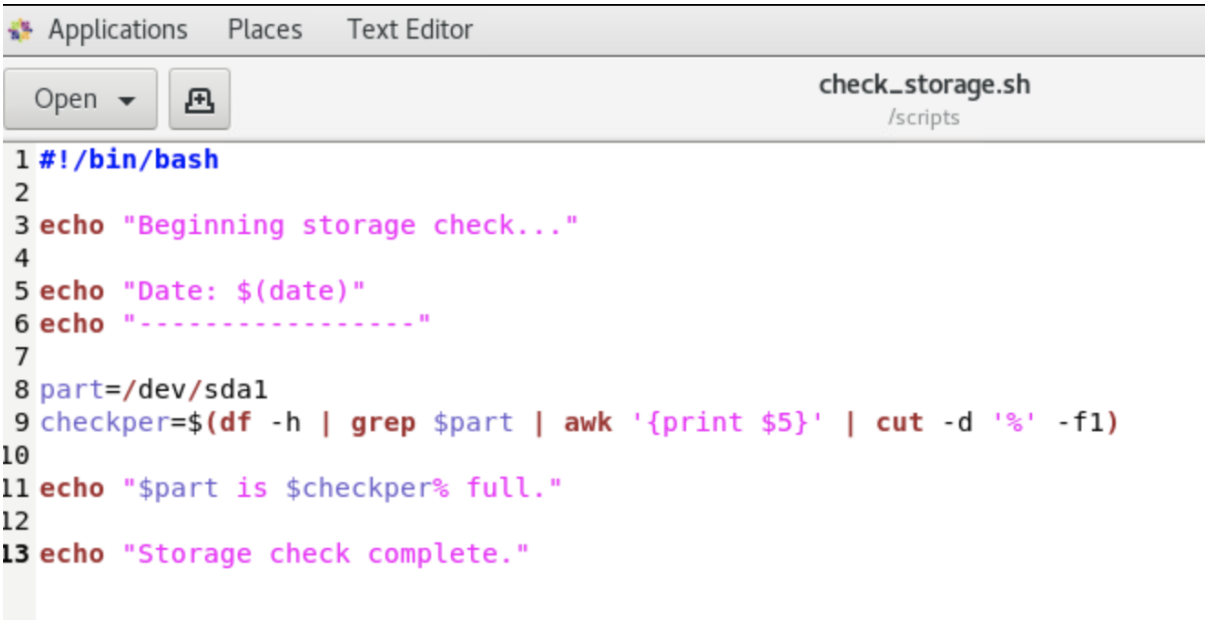
4. Assign the main variables the script will use
    - On a `new line 8`, type `part=/dev/sda1`
    - You're defining this variable so you can use it later as the name of the partition to check.
    - On a `new line 9`, type the following:
    - `checkper=$(df -h | grep $part | awk '{print $5}' | cut -d '%' -f1)`

- There's quite a bit being assigned to this variable. The following is a breakdown:
  - First, the entire value is a command, so it uses the command substitution format, i.e., `$(…)`
  - The first subcommand uses `df` to get drive information.
  - This is piped to the `grep` command, which searches the results for anything matching the `$part` variable you just defined (in this case, `/dev/sda1).`
  - The `awk` command extracts the data in the fifth column of these results. If you issue`df -h` by itself, you can see that the fifth column details the percentage of the storage device that is being used.
  - Lastly, the cut command simply strips the percent sign (`%`) from the value so that the script can perform arithmetic on it.
  - The ultimate result is just a single number that represents the percentage of storage being used by the `/dev/sda1` partition.



5. Write echo statements that report storage usage and indicate the check is complete

- On a new line 11, type the following:
- `echo "$part is $checkper% full."`
- On a new line 13, type the following:
- `echo "Storage check complete."`
- Select `Save`.



6. Test the script

- Switch to a terminal, but keep the text editor open.
- At the terminal, enter `check_storage.sh`
- Verify that the output displays the date and time, the percentage full message, and the completion message.

```
[student01@server01 ~]$ check_storage.sh
Beginning storage check...
Date: Wed Jan  2 16:00:41 GMT 2019
------------------
/dev/sda1 is 5% full.
Storage check complete.
```

7. Redirect the pertinent output to a file instead of the CLI

- Return to the text editor.
- Place your cursor at the end of line 3 and press Enter twice.
- On a new line 5, type the following:
- `exec >> ~/storage_report.txt`
- Now, all output in this script will be redirected to a file, unless otherwise specified.
- Change the echo statement on line 15 so that it reads:
- `echo "Storage check complete. Report saved to storage_report.txt." >&2`
- This will redirect the message to the CLI (through `stderr`) in order to bypass the `exec` command.
- Save the script.
- screenshot4

8. Test the script again

- From a terminal, run the script again.
- Verify that the only messages printed to the CLI are the beginning and completion messages.
- Enter `cat storage_report.txt` and verify that everything else was sent to this file.

```
[student01@server01 ~]$ cat storage_report.txt
Date: Wed Jan  2 16:03:09 GMT 2019
------------------
/dev/sda1 is 5% full.
```

- From a functionality perspective, how does this script fall short? How could it be improved? Click here for the answer.

Incorporating Conditional Statements in Bash Scripts

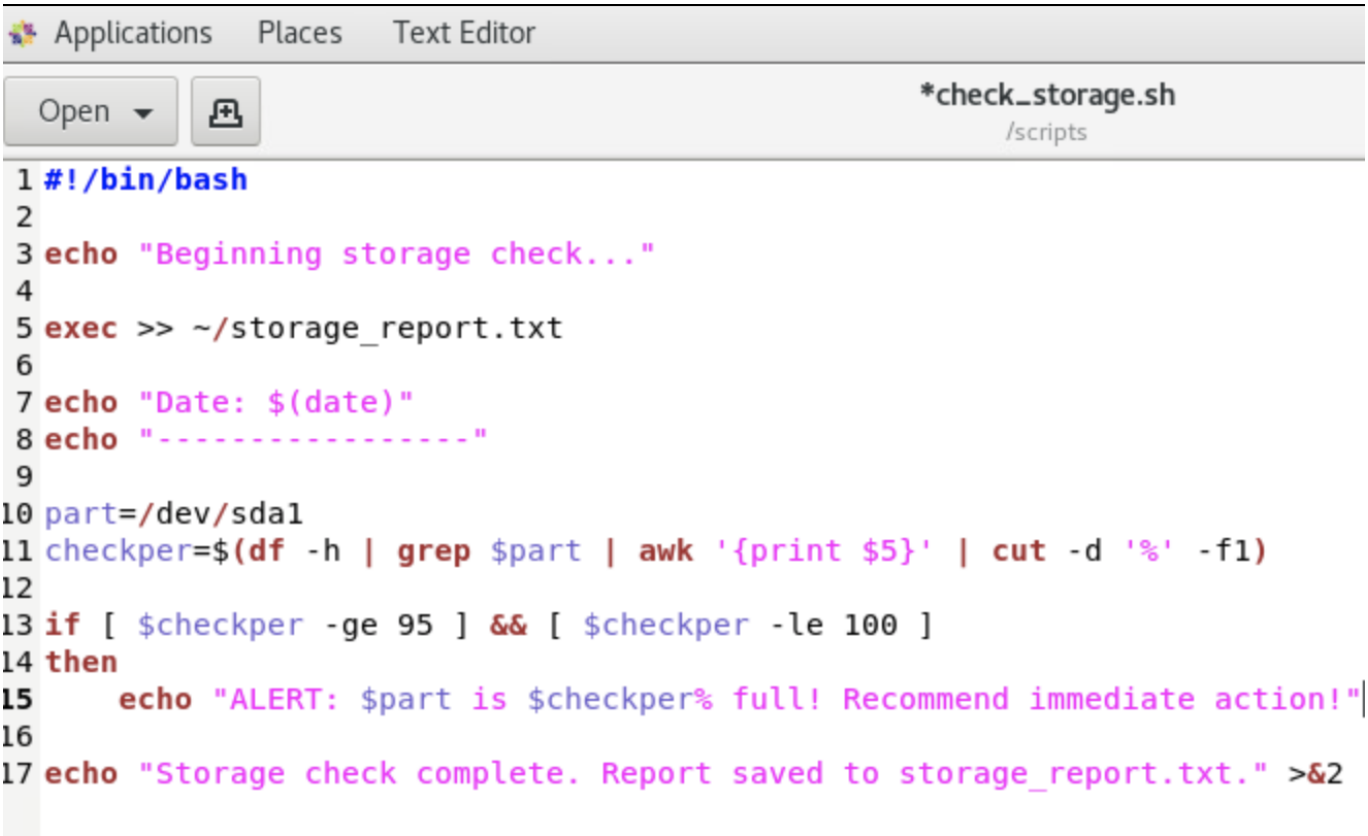
> Scenario

```
You want to make your script more useful to the administrators who will be
receiving the reports. You can do this by enabling the script to make decisions
based on various conditions. So, you'll use various if statements to output a
```

```
different message for when the storage device meets certain thresholds of
percentage full. Devices that are very close to full will trigger an urgent
message, whereas those that are less full will trigger less urgent messages.
```

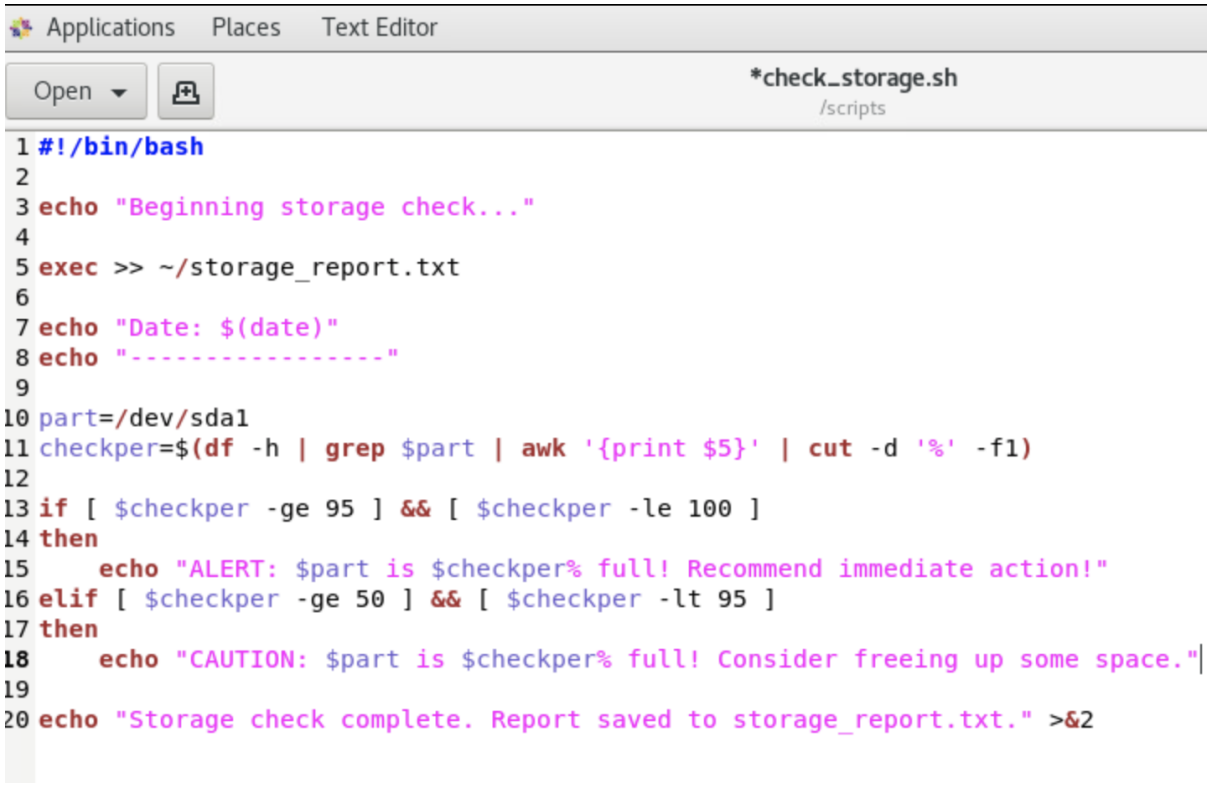
> Objectives Completing this activity will help you to use content examples from the following syllabus objectives: 5.1 Given a scenario, deploy and execute basic Bash scripts

1. Return to check_storage.sh in the text editor.
    - Place your cursor on the blank line 12 to start writing the first conditional branch.
    - Press `Enter`.
    - On a new line 13, type the following:
    - `if [ $checkper -ge 95 ] && [ $checkper -le 100 ]`
    - Press `Enter`.
    - On a new line 14, type `then`
    - Place your cursor at the beginning of line 15 and press `Spacebar` four times.
    - You're not required to indent or create whitespace, but it helps make the code more readable.
    - Modify the `echo` statement on line 15 to read like the following:
    - `echo "ALERT: $part is $checkper% full! Recommend immediate action!"`
    - You've just created the first if branch. This code checks to see if the percentage full value is greater than or equal to 95 and less than 100. If it is, then the script will `echo` an alert to the `storage_report.txt` file. However, you still need to write more branches to handle other conditions.



1. Write the next conditional branch
    - Place the cursor at the end of line 15 and press `Enter`.
    - On a new line 16, type the following:

- `elif [ $checkper -ge 50 ] && [ $checkper -lt 95 ]`
- Press `Enter`.
- On a new line 17, type `then`
- Press `Enter`.
- On a new line 18, indent and then type the following:
- `echo "CAUTION: $part is $checkper% full! Consider freeing up some space."`
- If the previous condition is not met, the script will move on to evaluating the condition in this elif branch. The condition here checks to see if the percentage full is greater than or equal to 50 and less than 95. If it is, then a different message will be echoed to the report file.

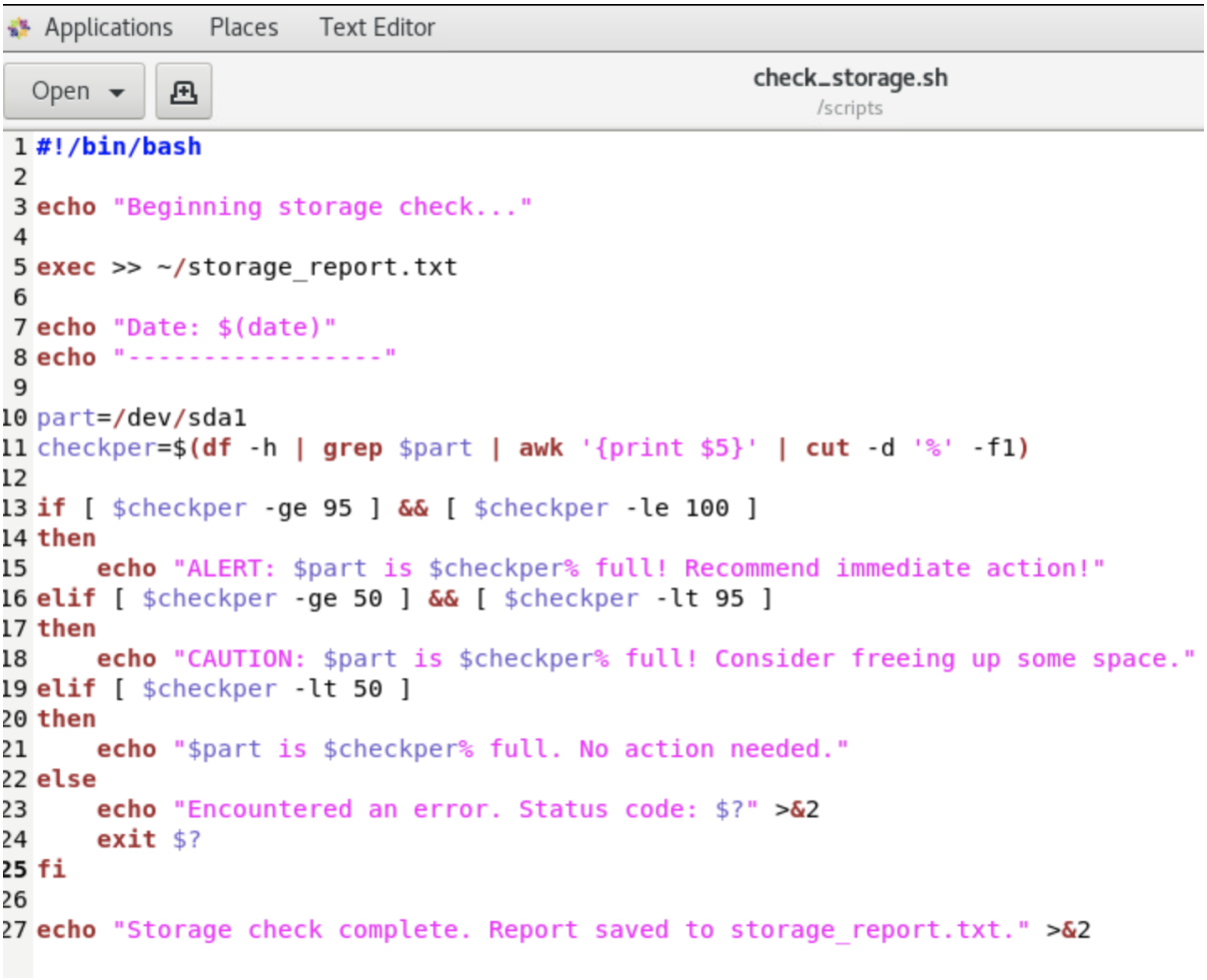


2. Finish writing the remaining conditional branches

- Press Enter.
- Starting on a new line 19, type the following code:

```
elif [ $checkper -lt 50 ]
then
echo "$part is $checkper% full. No action needed."
else
echo "Encountered an error. Status code: $?" >&2
exit $?
fi
```

- Indent lines 21, 23, and 24.
- The next branch will output another message if the percentage full is less than 50. If none of these conditions are met (i.e., the percentage value is above 100 or it isn't a number), then the last else branch will throw an error. That exit code will be printed to the CLI and the script will terminate with this code.
- Save the script.



3. Test the script to see if the conditions work as expected

   - From a terminal, enter check_storage.sh
   - Enter `cat storage_report.txt` and verify that, because `/dev/sda1` is not very full, the report indicates that no action is needed.

```
[student01@server01 ~]$ cat storage_report.txt
Date: Wed Jan  2 16:03:09 GMT 2019
------------------
/dev/sda1 is 5% full.
Date: Wed Jan  2 16:08:12 GMT 2019
------------------
/dev/sda1 is 5% full. No action needed.
```

   - In other words, the script chose the correct action to take based on the conditions you set.
     - You'll test some of the other conditions in the next activity.

Incorporating Loops in Bash Scripts

> Scenario

Your script is coming along, but it still needs improvement. You want to be able to output the status of all relevant storage partitions/volumes on the system, not just one or a few. You need a way to programmatically test your conditions for each device, rather than hardcode device names in your script—especially if the

storage devices are likely to change. So, you'll leverage a for loop to iterate over each recognized storage device to perform the necessary checks.

> Objectives Completing this activity will help you to use content examples from the following syllabus objectives: 5.1 Given a scenario, deploy and execute basic Bash scripts

1. Adjust the part variable so that it holds an array of device names

    - Place your cursor on line 10 where the part variable is defined.
    - Change this line to the following:
    - `part=$(df -h | awk '{print $1}' | grep '/dev')`
    - This is similar to the checkper variable. The difference is, it will extract all text that is in the first column (device name), and then filter by devices that start with `/dev` to exclude temporary file systems. The part variable therefore becomes an array that holds all permanent storage device names on the system.

```
 8 echo "-----------------"
 9
10 part=$(df -h | awk '{print $1}' | grep '/dev')
11 checkper=$(df -h | grep $part | awk '{print $5}' | cut -d '%' -f1)
```

2. Insert a for loop that will iterate through the part array

    - Place your cursor at the end of line 10, then press Enter twice.
    - On a new line 12, type the following:
    - `for i in ${part[*]}`
    - This begins the for loop. The i variable is the iterator. The part variable is being referenced as an array, with the asterisk (*) indicating all values in that array. For every index in the array (i.e., every device name), the script will execute what follows.
    - Press `Enter`, and on line 13, type `do`
    - This begins the code that the loop will execute on each iteration.
    - Place your cursor at the end of line 28 and press Ent`er.
    - On line 29, type `done`
    - This terminates the `for loop`. The conditional statements within this loop will be executed for each iteration.

```
11
12 for i in ${part[*]}
13 do
14 checkper=$(df -h | grep $part | awk '{print $5}' | cut -d '%' -f1)
15
16 if [ $checkper -ge 95 ] && [ $checkper -le 100 ]
17 then
18     echo "ALERT: $part is $checkper% full! Recommend immediate action!"
19 elif [ $checkper -ge 50 ] && [ $checkper -lt 95 ]
20 then
21     echo "CAUTION: $part is $checkper% full! Consider freeing up some space."
22 elif [ $checkper -lt 50 ]
23 then
24     echo "$part is $checkper% full. No action needed."
25 else
26     echo "Encountered an error. Status code: $?" >&2
27     exit $?
28 fi
29 done
30
```

3. Change $part references to use the iterator instead

- On line 14, change the `grep $part portion` of the command to `grep $i`
- You need to get the information for each device individually. This means you need to reference the iterator, not the entire array.
- On line 18, change the `$part` reference to `$i`
- Do the same for lines 21 and 24.

4. Clean up the source code

- Highlight all of lines 14 through 28.
- Press Tab to indent the selected lines.
- Save the file.

```
 9
10 part=$(df -h | awk '{print $1}' | grep '/dev')
11
12 for i in ${part[*]}
13 do
14         checkper=$(df -h | grep $i | awk '{print $5}' | cut -d '%' -f1)
15
16         if [ $checkper -ge 95 ] && [ $checkper -le 100 ]
17         then
18             echo "ALERT: $i is $checkper% full! Recommend immediate action!"
19         elif [ $checkper -ge 50 ] && [ $checkper -lt 95 ]
20         then
21             echo "CAUTION: $i is $checkper% full! Consider freeing up some space."
22         elif [ $checkper -lt 50 ]
23         then
24             echo "$i is $checkper% full. No action needed."
25         else
26             echo "Encountered an error. Status code: $?" >&2
27             exit $?
28         fi
29 done
30
31 echo "Storage check complete. Report saved to storage_report.txt." >&2
```

5. Test the script

- From a terminal, enter `check_storage.sh`
- Enter `cat storage_report.txt`
- Verify that the report lists all storage devices and their appropriate warning messages.

6. Simulate a volume becoming full, then test the script again

- At a terminal, enter `sudo dd if=/dev/zero of=/backup/sys/test bs=1M count=1100`
- Verify that roughly 1.2 GB was copied to the volume.
- Run your script again and read the report.
- Verify that, this time, you receive a caution warning because the volume is past 50% full.
- Enter `sudo dd if=/dev/zero of=/backup/sys/test2 bs=1M count=800`
  - The output file name and count have both changed.
- Run the script again and view the report.
- Verify that you received the most urgent message for the volume.
- Close the text editor, but keep the terminal open.

Automating Tasks

Scheduling a Single Task

> Scenario

Periodically, the developers at Develetech need to execute a task after hours. The schedule is not predictable and they need to be able to manage these tasks themselves. You will use the at command to satisfy this requirement.

> Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
    - 2.6 Given a scenario, automate and schedule jobs

Schedule a task to run for two minutes into the future from your current time

1. You will schedule a task that deletes a file from your home directory two minutes into the future.
    - Log in as `student01` with `Pa22w0rd` as the password.
    - In your home directory, use the `touch` command to create a file named `fileA`
    - Check the current time on your system by using the `date` command.
    - Enter at now + 2 minutes to access the interactive mode of the at command.
    - Enter `rm -f ~/fileA` and then press `Ctrl+D` to return to `Bash`.
    - Enter `atq` to view the scheduled job.
    - After two minutes, ensure that the command executed by checking the contents of your home directory to see if `fileA` was removed.

Scheduling Repeated Tasks

> Scenario

Develetech adopted a new policy that requires all users to fill in their time sheets every day. You'll create a daily reminder for all user systems.

> Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:

  > 2.6 Given a scenario, automate and schedule jobs

1. Schedule a cron job to email a reminder every day at a specified time

    - Enter `sudo crontab -u cmason -e` to specify a cron job for Chris Mason.
    - Verify that Vim opens a temporary file automatically.
    - Type the following line in the file:
    - `MM HH * * * /bin/echo "Please fill in your time sheet."`

- Replace `MM` and `HH` with the appropriate minute and hour time values in 24-hour time format. Ensure that the time you enter is three minutes ahead of the current system time. This way, you'll be able to see the message during the lab.
- For example, if the time is 2:30 P.M., you'd type:
- `33 14 * * * /bin/echo "Please fill in your time sheet."`
- Save and close the file.
- From the desktop menu, select the icons at the top-right, then select `student01→Log Out`.
- `Select Log Out`.

2. Verify that *Chris Mason* received the reminder for the scheduled job

- Log in as *Chris Mason*.
  - You can ignore the Welcome screen, or you can step through the wizard to dismiss it.
- Open a terminal.
- Wait for the time to pass for the cron job to execute.
- Remember, you can use date to check the time. You can also check the time from the desktop menu in the GUI.
- Enter `mail`
- Enter `1` to read the contents of the first email message.
- Verify that the mail contains a reminder to fill in the time sheet.
- Press `q` to quit the mail service.
- Log out as `Chris Mason` and log back in as your `student01` account.

Implementing Version Control Using Git

> Scenario

The development team needs a way to easily manage the different versions of the code they write. Multiple developers will be working in conjunction on the same project, so they need to a way to minimize conflicts while being able to revert to older versions of code, if necessary. So, you'll set up a Git repository for the developers so that they have a distributed version control system to work from.

> 5.2 Given a scenario, carry out version control using Git

1. Install and configure a Git repository

- Enter `sudo systemctl kill packagekit` to halt any updates the system may be doing.
- Enter `sudo yum -y install git --disablerepo=internal-repo` and wait for the installation process to complete.
- Enter `git config --global user.name 'Student User'`
- Enter `git config –-global user.email 'student01@develetech.com'`
- Create a directory in your home directory called dev-project and use the cd command to enter the directory.
- Enter `git init` to designate the dev-project directory as a Git repository.
- A message is returned from Git indicating the repository is initialized.
- Enter `ls -a` to view the `.git directory` created by the initialization process.

2. Create and manage a project using Git

- Use a text editor to create a file named `HelloWorld.txt`

- Enter the following text in the `HelloWorld.txt` file:
- `Hello, World! From Student01`
- Save your changes and close the editor.
- Enter git status to check the status of the `HelloWorld.txt` file.
- The file is marked as "Untracked", meaning it is not yet managed by Git.
- Enter `git add HelloWorld.txt` to enable Git to manage the file.
- Enter `git commit -m "Initial Commit"`
- This updates Git with the version information for the `HelloWorld.txt` file.
- Enter `git status` to check the status of the `HelloWorld.txt` file.
- The output indicates that there is nothing to commit because the `HelloWorld.txt` file version is now managed by Git.

3. Commit a change to the Git repository

-) Use a text editor to open the `HelloWorld.txt` document, and add the following on a new line:
- `Git version control test`
- Save your changes and close the editor.
- Enter `git status` and observe that Git reports the `HelloWorld.txt` file as modified, but that the changes are not yet committed to the repository.
- Enter `git add HelloWorld.txt` to stage the changes.
- Enter `git commit -m "Revision 1"` to commit the changes to the master copy of the file.
- Enter `git status` and notice that there are now no changes to commit to the repository.
- Enter `git log` to view the revision history of the repository.
- Times and dates for the initial commit and the revision have been logged.

Installing Linux

Scenario

Now that your preparations are complete, you're ready to install Linux on the various systems you selected. You'll start by installing CentOS 7 on the VM you created earlier. As you go through the installation, you'll configure various options so that the base environment will be automatically set up to your specifications.

Objectives

- Completing this activity will help you to use content examples from the following syllabus objectives:
  - 1.3 Given a scenario, configure and verify network connection parameters
  - 1.4 Given a scenario, manage storage in a Linux environment
  - 1.5 Compare and contrast cloud and virtualization concepts and technologies
  - 1.6 Given a scenario, configure localization options

1. Load the previously created VM
   - You will work with the VM you created in the previous exercise.
   - Log in as `student01` with `Pa22w0rd` as the password.
   - At a terminal, enter `sudo virsh restore saved-vm`
   - This restores the VM you created earlier from its saved state. This may impact the performance of your lab computer for a few minutes.
   - From the desktop menu, select `Applications→System Tools→Virtual Machine Manager`.
   - Enter the `root` password.
   - Right-click the `devtech-install VM` and select `Open`.
   - Wait for the installation media to finish its check. You can press `Esc` to skip the check, but it's wise to check the media at least once when setting up production systems.

2. Configure localization settings
   - If necessary, expand the virtual machine window so it's easier to see.
     - You can also select the `Switch to fullscreen view button`.
   - On the `WELCOME TO CENTOS 7` page, select `Continue` to accept the default language settings.
   - On the INSTALLATION SUMMARY page, under the `LOCALIZATION` section, select `DATE & TIME`.
   - Select your time zone, then select Done.

3. Select the software components and base environment to install
   - Under the `SOFTWARE` section, select `SOFTWARE SELECTION`.
   - From the Base Environment list, select `Server with GUI`.
   - From the Add-Ons for Selected Environment list, check the `KDE` check box.
   - By default, the Server with GUI selection will install most tools necessary for the configuration and maintenance of general server infrastructure, along with `GNOME` as the default GUI. You're

also installing KDE alongside that for users to have a choice of desktop environment.
- Select Done.

4. Wipe the storage device to start fresh

- Under the SYSTEM section, select INSTALLATION DESTINATION.
- On the Device Selection page, observe the Virtio Block Device.
- This is the 12 GB virtual storage device that was created when you first installed the VM.
- Under Other Storage Options, ensure Automatically configure partitioning is selected.
- Check the I would like to make additional space available check box.
- Select Done.
- In the RECLAIM DISK SPACE dialog box, verify that the vda device is selected, and that it has 12 GB of free space. This is because the virtual storage device you created is currently empty. Still, it's useful to practice wiping a storage device in order to start fresh.
- Select Delete all.
- Select Reclaim space.

5. Configure the partitioning scheme to use

- On the INSTALLATION SUMMARY page, select INSTALLATION DESTINATION again.
- Under Other Storage Options, select I will configure partitioning.
- Select Done.
- Under New CentOS 7 Installation, verify that no mount points have been created yet, and that the default partitioning scheme will use LVM.
- Select Click here to create them automatically.
- Verify that three partitions/volumes were created: /boot, / (root), and swap. Notice that there is no separate /home volume. This is because the CentOS 7 installer only creates a separate /home volume by default when the storage device is 50 GB or more. In this case, the /home directory will be located within the root volume.
- Select the /boot partition and note its default capacity, device type (partitioning scheme), and file system type.
- Select the / (root) volume and the swap volume and note their defaults as well.
- These will be created as logical volumes within the centos volume group.
- At the bottom-left of the page, note the total space of the storage device as well its available space.
- This reflects the intended partitioning scheme; no changes will be made to the drive until installation begins in earnest.
- Select Done.
- In the SUMMARY OF CHANGES dialog box, select Accept Changes.

6. Configure networking

- On the INSTALLATION SUMMARY page, select NETWORK & HOST NAME.
- In the Host name text box at the bottom-left, type devtech-vm01 then select Apply.
- In the list of devices on the left, verify that Ethernet (eth0) is selected.
- This is the virtual network interface that was created for the VM to use.
- Select Configure at the bottom-right of the page.
- In the Editing eth0 dialog box, select the IPv4 Settings tab.

- From the Method drop-down list, select `Manual.`
- To the right of the Addresses list, select the `Add` button.
- For the Address, type `10.50.1.201`
  - Your lab environment might require different addresses than those listed in these steps.
- Press Tab, then for the Netmask, type `255.255.255.0`
- Press Tab, then for the Gateway, type `10.50.1.1` and press Enter.
- In the DNS Servers text box, type `8.8.8.8`
- Select `Save.`
- Select the slider at the top-right to turn the interface On.
- Verify that the interface details are as you expect, then select`Done`.

7. Begin installation and configure user accounts

- Select Begin Installation.
- Observe the progress bar at the bottom, indicating that `CentOS` is in the process of being installed.
- Under `USER SETTINGS,` select `ROOT PASSWORD`.
- In the Root Password text box, type `Pa22w0rd`
- In the Confirm text box, type`Pa22w0rd`
- Select `Done`, then, at the bottom of the screen, verify that`CentOS` points out that this password is weak because it's based on a dictionary word. In a production environment, you'd want to choose a much stronger password.
- Select `Done` again to agree to use the password.
- Select `USER CREATION`.
- In the User name text box, type `student01`
- Check the `Make this user administrator` check box.
- In the `Password` and `Confirm password` text boxes, type `Pa22w0rd`
- Select Done twice to confirm the password.
- In addition to creating a stronger password, you'd also want to make your user password different than the root password in a production environment.
- Wait for the system to finish installing.
  - The remainder of the installation process may take up to 30 minutes.

8. Complete the installation process

- When installation finishes, select `Reboot`.
- From the `VM` window, select `Virtual Machine→Run` to restart the `VM`.
- On the `INITIAL SETUP` page, select `LICENSING INFORMATION`.
- Check I accept the license agreement and select Done.
- Select `FINISH CONFIGURATION`.
- Verify that you are greeted with the sign in screen, indicating that `CentOS 7` was successfully installed.

9. Verify your new system's configurations

- Sign in as your student account.
- Using what you've learned, check the `VM` for the following:

```
        - Storage partition and logical volume configurations.
        - User accounts.
        - Networking configurations.
        - Connectivity with other classroom computers.
        - Internet connectivity.
        - Additional software packages.
```

- When you're done, from the `VM` window, select `Virtual Machine→Shut Down→Shut Down`.
- Close the VM window.