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.