Activity overview

Previously, you focused on authorization, the concept of granting access to specific resources in a system. Another important concept in security is authentication. Authentication is the process of a user proving that they are who they say they are in the system.

When managing this, security analysts need to ensure

- not all users get access to the system,
- new users (those who are new to the organization or a group) are added to the system, and
- current users who change groups or leave the organization are deleted from the system.

In this lab activity, you'll use the `useradd`, `usermod`, `userdel`, and `chown` commands to manage user access in the Linux Bash shell.

Important: You must use `sudo` at the beginning of all the commands you use in this lab. Adding or removing users and groups are tasks that require root (super user) privileges, and you'll need to use `sudo` with the commands that are used to perform these tasks.

Scenario

In this scenario, a new employee with the username `researcher9` joins an organization. You have to add them to the system and continue to manage their access during their time with the organization.

Here's how you'll do this task: **First**, you'll add a new employee to the system and then to their primary group. **Second**, you'll make this employee the owner of a file related to a particular project. **Third**, you'll add the new employee to a supplementary group. **Finally**, you'll delete the employee from the system.

Note: *The lab starts with you logged in as user `analyst`, with your home directory, `/home/analyst`, as the current working directory.*
OK, it's time to get ready to practice managing user access in Linux!

Disclaimer: For optimal performance and compatibility, it is recommended to use either **Google Chrome** or **Mozilla Firefox** browsers while accessing the labs.

Start your lab

You'll need to start the lab before you can access the materials. To do this, click the green "Start Lab" button at the top of the screen.

Start Lab

After you click the **Start Lab** button, you will see a shell, where you will be performing further steps in the lab. You should have a shell like this:

When you have completed all the tasks, refer to the End your Lab section that follows the tasks for information on how to end your lab.

Task 1. Add a new user

A new employee has joined the Research department. In this task, you must add them to the system. The username assigned to them is `researcher9`.

1. Write a command to add a user called `researcher9` to the system.

The command to complete this step:

```
sudo useradd researcher9
```

Copied!

content_copy

Next, you need to add the new user to the `research_team` group.

2. Use the `usermod` command and `-g` option to add `researcher9` to the `research_team` group as their primary group.

The command to complete this step:

```
sudo usermod -g research_team researcher9
```

Copied!

content_copy

You could alternatively use the following variation of `useradd` when creating the user to perform both steps at once:

```
sudo useradd researcher9 -g research_team
```

Copied!

content_copy

Click **Check my progress** to verify that you have completed this task correctly.

Add a new user

Check my progress

Task 2. Assign file ownership

The new employee, `researcher9`, will take responsibility for `project_r`. In this task, you must make them the owner of the `project_r.txt` file.

The `project_r.txt` file is located in the `/home/researcher2/projects` directory, and owned by the `researcher2` user.

- Use the `chown` command to make `researcher9` the owner of `/home/researcher2/projects/project_r.txt`.

The command to complete this step:

```
sudo chown researcher9 /home/researcher2/projects/project_r.txt
```

Copied!

content_copy

Click **Check my progress** to verify that you have completed this task correctly.

Assign file ownership

Check my progress

Task 3. Add the user to a secondary group

A couple of months later, this employee's role at the organization has changed, and they are working in both the Research and the Sales departments.

In this task, you must add `researcher9` to a secondary group (`sales_team`). Their primary group is still `research_team`.

- Use the `usermod` command with the `-a` and `-G` options to add `researcher9` to the `sales_team` group as a secondary group.

The command to complete this step:

```
sudo usermod -a -G sales_team researcher9
```

Copied!

content_copy

Note: *Options for Linux commands are case-sensitive, so make sure you use a lowercase `-a` and an uppercase `-G`.*
Click **Check my progress** to verify that you have completed this task correctly.

Add the user to a secondary group

Check my progress

Task 4. Delete a user

A year later, `researcher9`, decided to leave the company. In this task, you must remove them from the system.

1. Run a command to delete `researcher9` from the system:

```
sudo userdel researcher9
```

Copied!

content_copy

This command will output the following message:

```
Userdel: Group researcher9 not removed because it is not the primary group of user researcher9.
```

This is expected.

Note: *When you create a new user in Linux, a group with the same name as the user is automatically created and the user is the only member of that group. After removing users, it is good practice to clean up any such empty groups that may remain behind.*

2. Run the following command to delete the `researcher9` group that is no longer required:

```
sudo groupdel researcher9
```

Copied!

content_copy

Click **Check my progress** to verify that you have completed this task correctly.

Delete a user

Check my progress

Conclusion

Great work!

You now have practical experience in using basic Linux Bash shell commands to

- add a new user,
- add a user to a group,
- change user permissions on files, and
- delete a user.

This is an important milestone on your journey toward managing users in Linux!