

# User Management in Linux

## Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of a system administrator for an organization responsible for user management. In this scenario, a new employee with the username **researcher9** joins the organization. Responsibilities include adding them to the system and continuing to manage their access during their time with the organization.

## Adding a new user

**Direction:** A new employee has joined the Research department. In this task, they must be added to the system. The username assigned to them is **researcher9**.

The **sudo** command was used for elevated superuser privileges to execute tasks. The **useradd** command was used to add **researcher9** to the system, followed by adding them to the group **research\_team** using the **usermod** command as follows:

```
analyst@cf52dea393f1:~$ sudo useradd researcher9
analyst@cf52dea393f1:~$ sudo usermod -g research_team researcher9
analyst@cf52dea393f1:~$
```

## Assigning File Ownership

**Direction:** The new employee, **researcher9**, will take responsibility for **project\_r**. In this task, they should be made owner of the **project\_r.txt** file.

The **sudo** command was used for elevated superuser privileges to execute tasks. The **chmod** command was used to transfer the ownership of **project\_r.txt** to **researcher9** as follows:

```
-rw-rw-r-- 1 researcher2 research_team 46 Aug 29 09:39 project_r.txt
```

## Adding user to secondary group

**Direction:** 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.

The user **researcher9** must now be added to a secondary group (**sales\_team**). Their primary group is still **research\_team**.

The **sudo** command was used for elevated superuser privileges to execute tasks. The **usermod** command was used along with the **-a** and **-G** options to add **researcher9** to the **sales\_team** group as a secondary group as follows:

```
analyst@cf52dea393f1:/home/researcher2/projects$ sudo usermod -a -G sales_team researcher9
```

## Deleting a user

**Direction:** A year later, **researcher9** decided to leave the company. They must now be removed from the system.

The **sudo** command was used for elevated superuser privileges to execute tasks. The **userdel** command was used to delete the user from the system as follows:

```
analyst@cf52dea393f1:/home$ sudo userdel researcher9
userdel: group researcher9 not removed because it is not the primary group of user researcher9.
```

It is observed that a group named **researcher9** is still not removed. This is because 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.

To rectify this, the **groupdel** command is used to remove the leftover group as follows:

```
analyst@cf52dea393f1:/home$ sudo groupdel researcher9
```

## Summary

User management was successfully performed in Linux using the **sudo**, **useradd**, **usermod**, **userdel**, and **groupdel** commands. All tasks were successfully completed in accordance to the directions given by the organization.