Managing Users, Groups & Permissions.

Scenario: *As a Linux System Administrator, you are responsible for creating user accounts, managing groups, and modifying permissions according to company requirements.*

Your company has tasked you with creating 3 new user accounts for the new hires. You have also been asked to create 3 groups for the new departments that have been established. And finally, in order to adhere to data privacy and compliance regulations, you need to ensure that the right permissions are put in place.

Objective

In this article I will be showing you how to create user accounts, groups, directories, and files, as well as how to properly set up and assign permissions in a Linux Server environment.

SECTION 1: Creating Directories and Files

Step 1

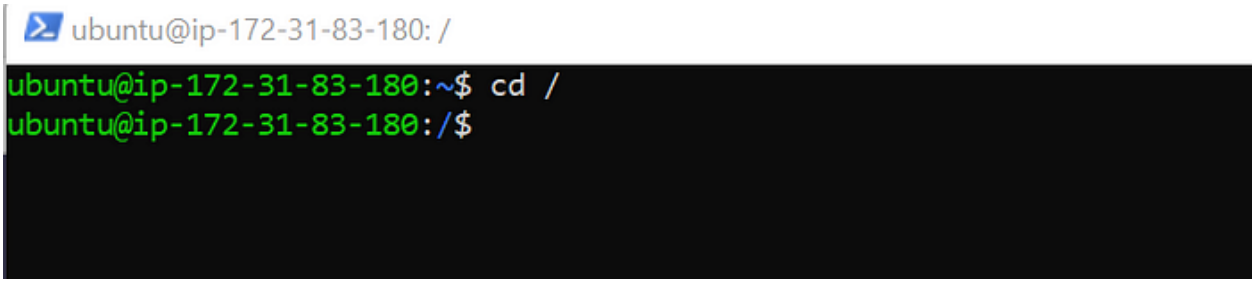
The very first step will be to connect to your Linux (Ubuntu) Instance via the Terminal. You can use any terminal of your choice.

Step 2

Now that you're logged into the instance, and you have the Linux server up and running, the next thing to do is to log in to the server's root directory. To do this, type in the following command:

```
cd /
```

This should be the result on your terminal.



Step 3

In this step, I would like to introduce you to the "***sudo***" command.

The `sudo` command in Linux stands for "Super User DO". It allows a user to have temporary administrative privileges in order to perform certain tasks.

We will be using this command quite frequently during this exercise.

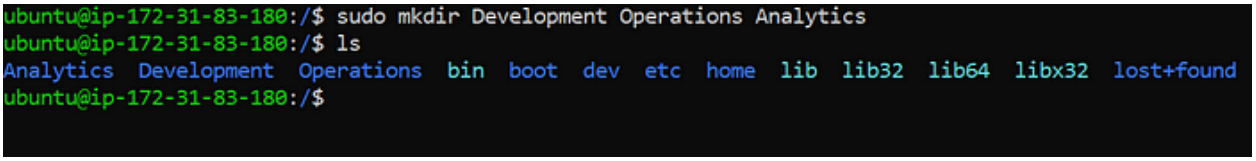
Step 4

Now we will be making 3 directories (folders). Folders are referred to as directories in a Linux environment.

To make directories we will be using the "***mkdir***" command. I will name my directories Development, Operations, and Analytics. You can also use these names for your directories, or you can choose different names.

```
sudo mkdir Development Operations Analytics
```

Now if you run the "ls" command, you should see your directories are successfully created.



Step 5

Next, we will create 3 files for each directory. You can create files in any format of your choice, such as .txt, .docx, .csv, .xls and so on.

Note: File names are case sensitive, meaning “dev.txt” is different from “Dev.txt”

To create files, we can make use of the “***touch***” command.

Don’t forget to use the “***sudo***” command as well, you will get a “Permission denied” error otherwise.

Starting with the Development directory, type in the following commands.

```
cd Development/

sudo touch myDevFile.txt devfile.docx devSheet.csv
```

Now if you run the “ls” command, you should see your files are successfully created.

```
ubuntu@ip-172-31-83-180:/Development$ ls
devSheet.csv  devfile.docx  myDevFile.txt
ubuntu@ip-172-31-83-180:/Development$
```

We’ll do the same for the Operations Directory.

```
cd ../Operations/

sudo touch OpsSheet.csv Opsfile.docx myOpsFile.txt
```

```
ubuntu@ip-172-31-83-180:/Operations$ ls
OpsSheet.csv  Opsfile.docx  myOpsFile.txt
ubuntu@ip-172-31-83-180:/Operations$
```

And finally for the Analytics Directory

```
ubuntu@ip-172-31-83-180:/Operations$ cd ../Analytics/
ubuntu@ip-172-31-83-180:/Analytics$ sudo touch numbers.txt myNumbers.csv numbersfile.docx
ubuntu@ip-172-31-83-180:/Analytics$ ls
myNumbers.csv  numbers.txt  numbersfile.docx
ubuntu@ip-172-31-83-180:/Analytics$
```

SECTION 2: Creating & Managing Groups

In this section we will be creating new groups, assigning directories to the groups, and assigning permissions to the groups.

Step 1

We can create groups using the command "***groupadd***". I will name my groups Developers, Operations, and Data Analysts. Again, you can name your groups as you wish.

```
sudo groupadd Developers
```

```
sudo groupadd Operations
```

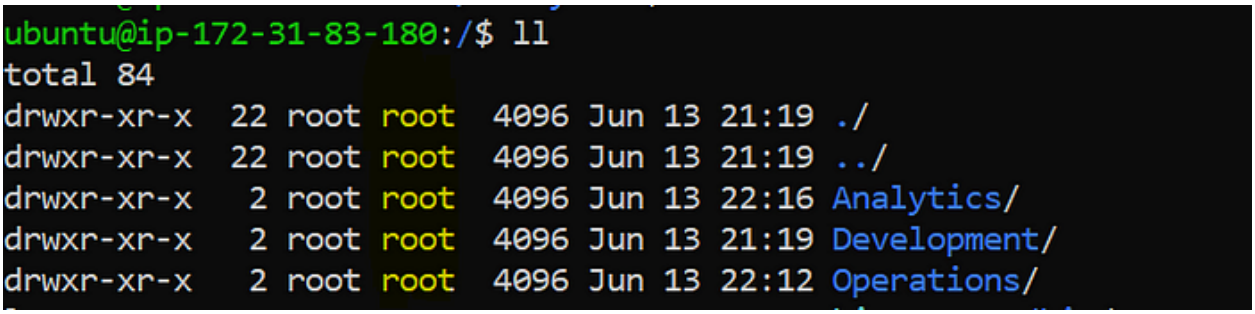
```
sudo groupadd Data_Analysts
```

Step 2

Next, I will assign the directories we created earlier to the new groups. One group per directory.

To do this, I can use the "***chown***" command. The "***chown***" command allows you to change the group owner of a file or directory.

If we run the `ll` command on the server's root directory, we will notice that the current group owner of our directories is the root user.



The yellow characters in the picture above indicate the current group owner of the directories.

Type in this command format to change the group owner of your directories.

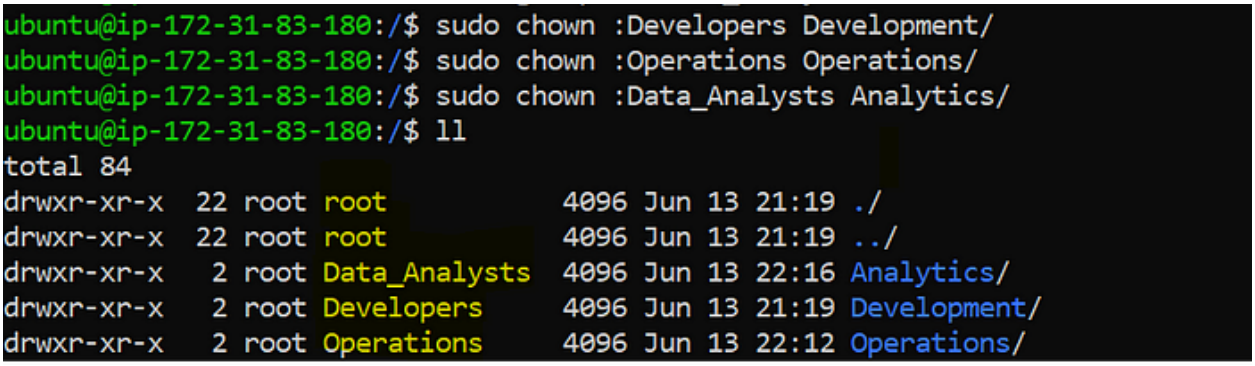
```
chown :GroupName DirectoryName
```

```
sudo chown :Developers Development/
```

```
sudo chown :Operations Operations/
```

```
sudo chown :Data_Analysts Analytics/
```

Now, if we run the `ll` command,



We have successfully updated the group owners of the directories.

Step 3

In this step we will be adding permissions for the directories to the groups according to company requirements.

Regarding permissions, there are 3 permissions that can be assigned.

1. r (read permissions)
2. w (write permissions)
3. x (execute permissions)

These permissions can be assigned to the following.

1. u (user owner)
2. g (group owner)
3. o (others)
4. a (all)

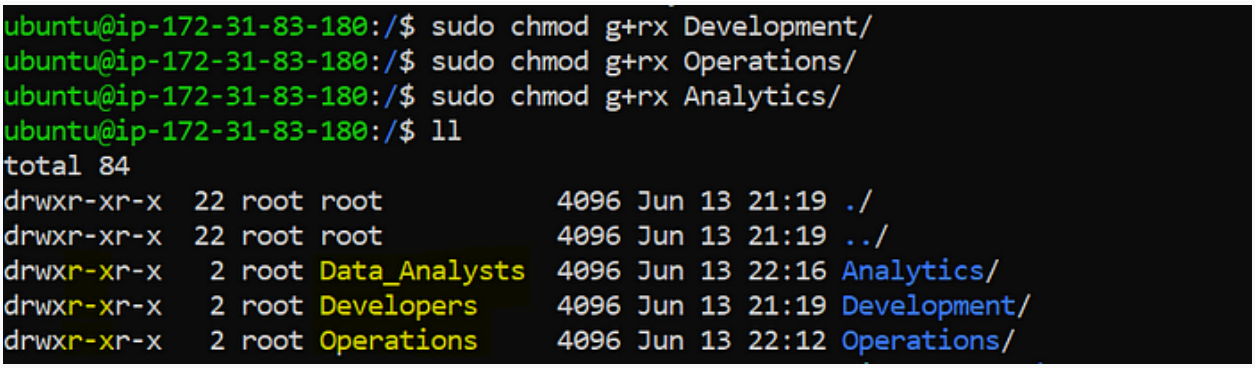
Company Requirements: Assign only read and execute permissions to the groups.

We can assign permissions for the directories to the groups using the "***chmod***" command.

```
sudo chmod g+rx Development/
```

```
sudo chmod g+rx Operations/
```

```
sudo chmod g+rx Analytics/
```



SECTION 3: Creating and Managing User Accounts

In this section, we will be creating new user accounts and assigning them to their respective groups according to company requirements.

***Company Requirements**: Create the following users and assign them to their respective groups.*

1. Jess Waller, username= jwaller,

email=jwaller@levelupbank.com, group= Developers

2. Blake Dorsey, username= bdorsey,

email=bdorsey@levelupbank.com, group= Operations

3. Joey Ewart, username= jewart,

email=jewart@levelupbank.com, group= Data Analysts

To create user accounts, we will use the command "***useradd***".

We will also make use of a few options when creating our users.

1. **-c** option is used to add text string. It is generally a short description of the login, and can be used for the user's full name, email address, contact number etc.
2. **-G** is used to assign the user to the specified group
3. **-m** is used to create the user's home directory if it does not exist.

```
sudo useradd username -c "Comments" -G groupname -m
```

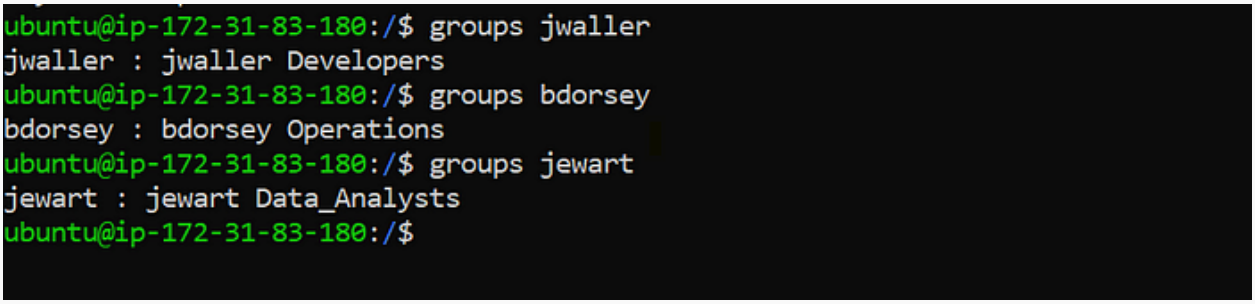
```
sudo useradd jwaller -c "Jess Waller, email=jwaller@levelupbank.com" -G Developers -m
```

```
sudo useradd bdorsey -c "Blake Dorsey, email=bdorsey@levelupbank.com" -G Operations -m
```

```
sudo useradd jewart -c "Joey Ewart, email=jewart@levelupbank.com" -G Data_Analysts -m
```

To confirm our user accounts were added to their respective groups, we can run the following command.

```
groups username
```



In the picture above, we can see that the user account for Jess Waller (jwaller) has been created and added to the Developers group, Blake Dorsey (bdorsey) has been created and added to the Operations group, and Joey Ewart (jewart) has been created and added to the Data Analysts group.

Success!!!

SECTION 4: Switching Users & Verifying Permissions

In this section, we will be switching to each of our newly created user accounts and verify that they are only able to see the directories associated with their group.

Company Requirements: *Users should only be able to see the directories associated with their group.*

Step 1

In order to ensure that users outside a group cannot access the directories and files associated with that particular group, we will need to remove the permissions.

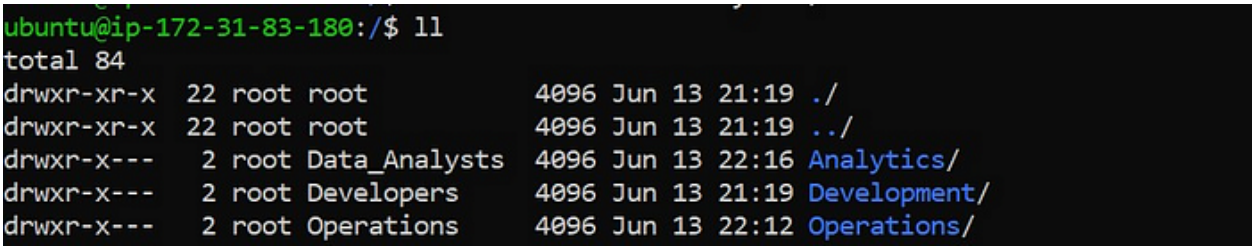
To remove the permissions for other users from the directories we created earlier, run the commands below.

```
sudo chmod o=- Development/
```

```
sudo chmod o=- Operations/
```

```
sudo chmod o=- Analytics/
```

The permissions are now updated.



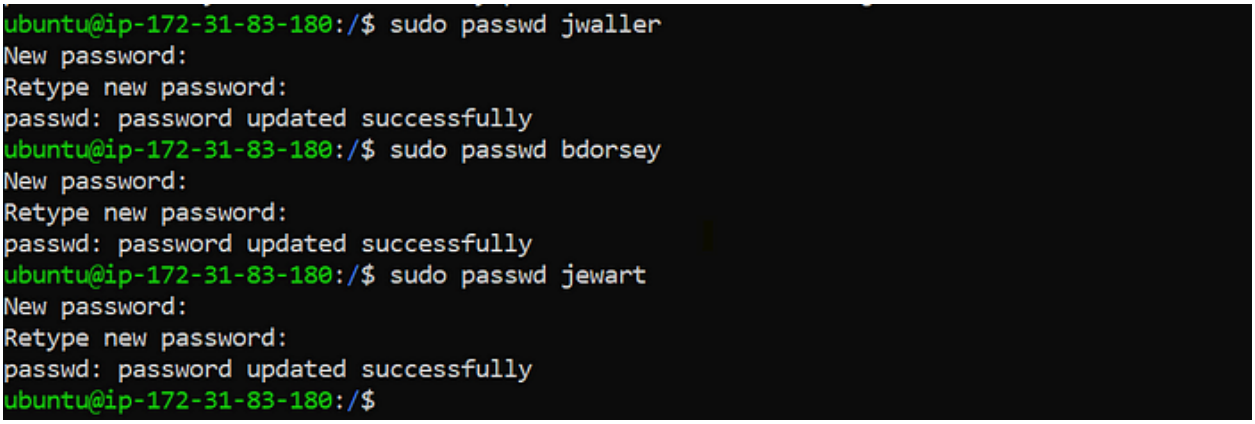
Step 2

Now, before we can switch users, we need to set passwords for the user accounts. To do this, we can use the "***passwd***" command.

Type in the command below.

```
sudo passwd username
```

Then type in the password for the user account.



Passwords have been set successfully.

Step 3

Now on to switching users.

To switch users, we use the "***su***" command, which simply means "switch user".

```
su - username
```

Type in the password for the user account, press enter, and then type in "**bash**". Now you've successfully logged in as the new user.

```
ubuntu@ip-172-31-83-180:/$ su - jwaller
Password:
$ bash
jwaller@ip-172-31-83-180:~$
```

Step 4

This step is all about verifying permissions for users.

For User Account: jwaller

The picture below shows that the user "***jwaller***" is able to access the Development directory because she is in the Developers group, but she is not able to access the Analytics or the Operations directory because she is not in the appropriate groups.

```
jwaller@ip-172-31-83-180:~$ cd /
jwaller@ip-172-31-83-180:/$ ls
Analytics  Development  Operations  bin  boot  dev  etc  home  lib  lib3
jwaller@ip-172-31-83-180:/$ cd Development/
jwaller@ip-172-31-83-180:/Development$ ls
devSheet.csv  devfile.docx  myDevFile.txt
jwaller@ip-172-31-83-180:/Development$ ll
total 8
drwxr-x---  2 root Developers 4096 Jun 13 21:19 ./
drwxr-xr-x 22 root root       4096 Jun 13 21:19 ../
-rw-r--r--  1 root root          0 Jun 13 17:36 devSheet.csv
-rw-r--r--  1 root root          0 Jun 13 17:36 devfile.docx
-rw-r--r--  1 root root          0 Jun 13 17:36 myDevFile.txt
jwaller@ip-172-31-83-180:/Development$ cd ../Analytics/
bash: cd: ../Analytics/: Permission denied
jwaller@ip-172-31-83-180:/Development$ cd ../Operations/
bash: cd: ../Operations/: Permission denied
```

For User Account: bdorsey

The picture below shows that the user "***bdorsey***" is able to access the Operations directory because he is in the Operations group, but he is not able to access the Analytics or the Development directory because he is not in the appropriate groups.

```
ubuntu@ip-172-31-83-180:/$ sudo su - bdorsey
$ bash
bdorsey@ip-172-31-83-180:~$ cd /
bdorsey@ip-172-31-83-180:/$ ls
Analytics  Development  Operations  bin  boot  dev  etc  home  lib  lib32  lib64  l
bdorsey@ip-172-31-83-180:/$ groups bdorsey
bdorsey : bdorsey Operations
bdorsey@ip-172-31-83-180:/$ cd Operations/
bdorsey@ip-172-31-83-180:/Operations$ ls
OpsSheet.csv  Opsfile.docx  myOpsFile.txt
bdorsey@ip-172-31-83-180:/Operations$ ll
total 8
drwxr-x---  2 root Operations 4096 Jun 13 22:12 ./
drwxr-xr-x 22 root root       4096 Jun 13 21:19 ../
-rw-r--r--  1 root root          0 Jun 13 22:12 OpsSheet.csv
-rw-r--r--  1 root root          0 Jun 13 22:12 Opsfile.docx
-rw-r--r--  1 root root          0 Jun 13 22:12 myOpsFile.txt
bdorsey@ip-172-31-83-180:/Operations$ cd ../Analytics/
bash: cd: ../Analytics/: Permission denied
bdorsey@ip-172-31-83-180:/Operations$ cd ../Development/
bash: cd: ../Development/: Permission denied
```

For User Account: jewart

The picture below shows that the user "***jewart***" is able to access the Analytics directory because he is in the Data Analysts group, but he is not able to access the Development or the Operations directory because he is not in the appropriate groups.

```
ubuntu@ip-172-31-83-180:/$ sudo su - jewart
$ bash
jewart@ip-172-31-83-180:~$ cd /
jewart@ip-172-31-83-180:/$ ls
Analytics  Development  Operations  bin  boot  dev  etc  home  lib  lib32
jewart@ip-172-31-83-180:/$ groups jewart
jewart : jewart Data_Analysts
jewart@ip-172-31-83-180:/$ cd Analytics/
jewart@ip-172-31-83-180:/Analytics$ ls
myNumbers.csv  numbers.txt  numbersfile.docx
jewart@ip-172-31-83-180:/Analytics$ ll
total 8
drwxr-x---  2 root Data_Analysts 4096 Jun 13 22:16 ./
drwxr-xr-x 22 root root          4096 Jun 13 21:19 ../
-rw-r--r--  1 root root             0 Jun 13 22:16 myNumbers.csv
-rw-r--r--  1 root root             0 Jun 13 22:16 numbers.txt
-rw-r--r--  1 root root             0 Jun 13 22:16 numbersfile.docx
jewart@ip-172-31-83-180:/Analytics$ cd ../Development/
bash: cd: ../Development/: Permission denied
jewart@ip-172-31-83-180:/Analytics$ cd ../Operations/
bash: cd: ../Operations/: Permission denied
```

This brings us to the end of the project.

You have successfully completed all the tasks assigned to you by the company. You met all of the company's requirements and adhered to data privacy and compliance regulations.