**DAWS\_81S**

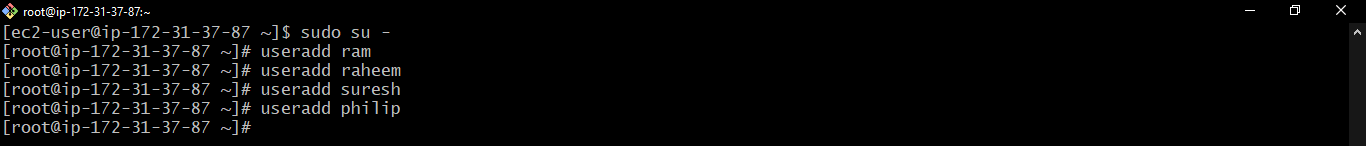
**ASSIGNMENT\_01**

**User and Group Management with Key-Based Authentication**

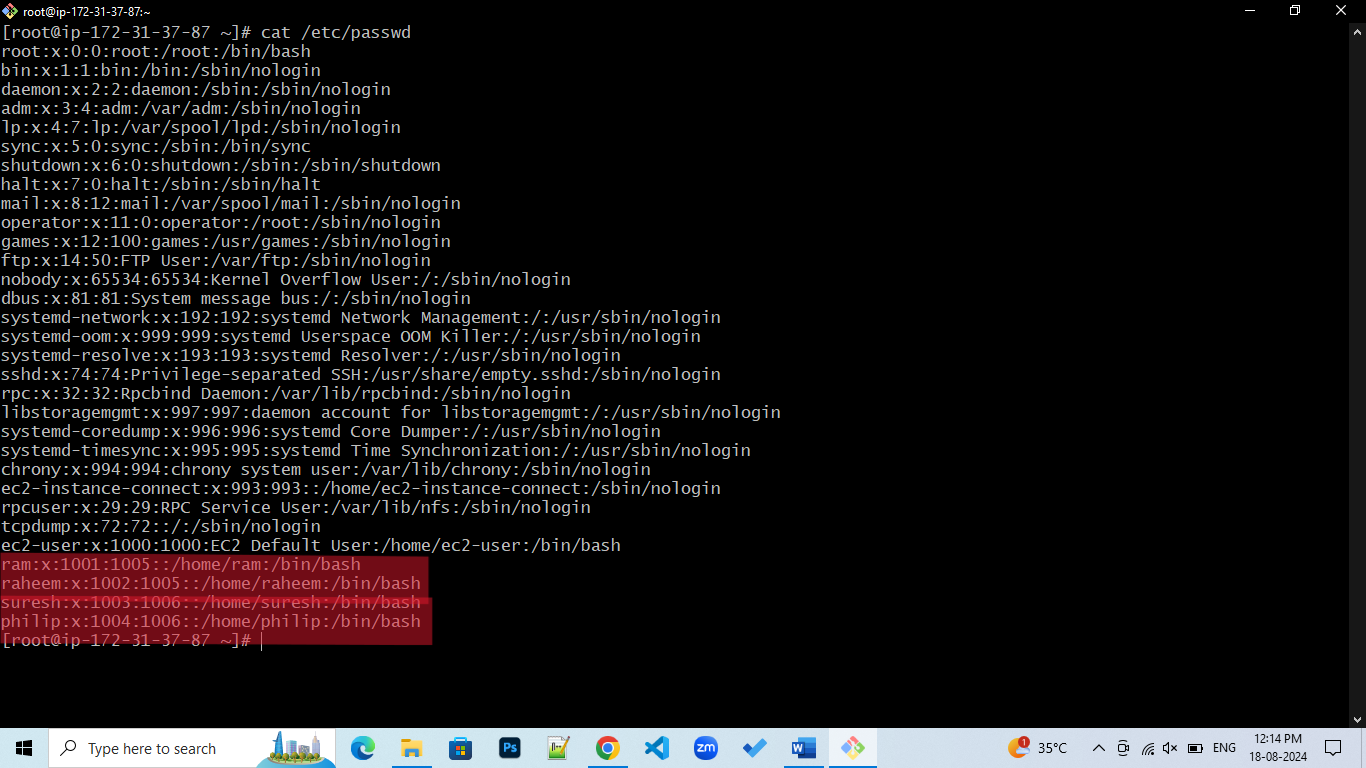
1. **User Creation**

First, we need to take the **root access** using the command **sudo su –** and then create users for Ram, Raheem, Suresh & Philip.

For user creation we use the command, **useradd <username>**



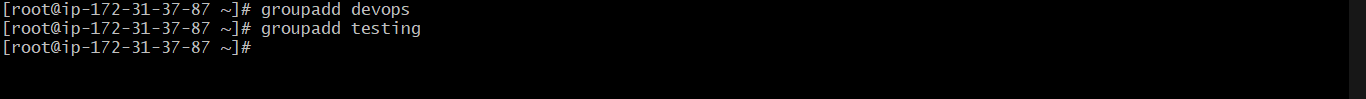
To check the user creation, go to **/etc/passwd** file.



1. **Group Creation**

Now, we will have to create two groups with names devops & testing.

For group creation we use the command, **groupadd <groupname>**



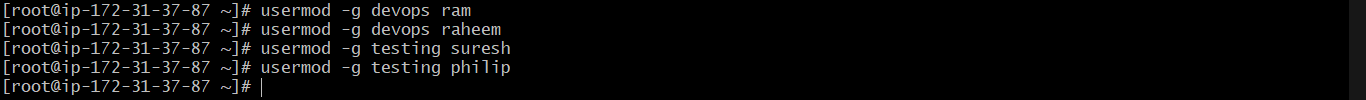
To check the group creation, go to **/etc/group** file.



1. **Assigning users to groups**

Now, we need to assign ram & Raheem to devops group, suresh & Philip to testing group.

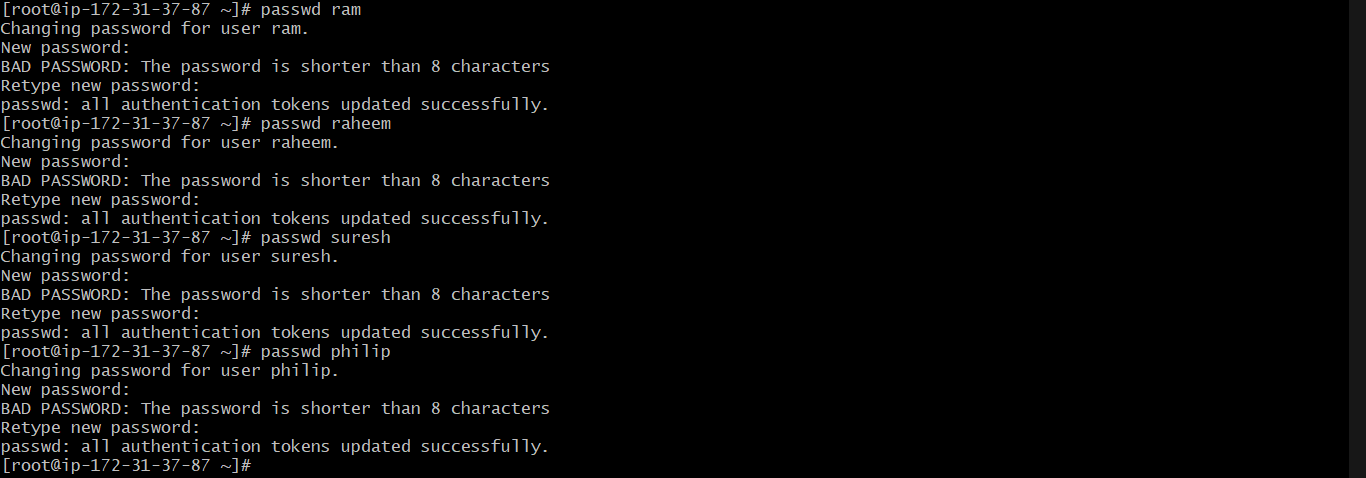
For assigning users to groups, we use the command, **usermod -g <groupname> <username>**

****

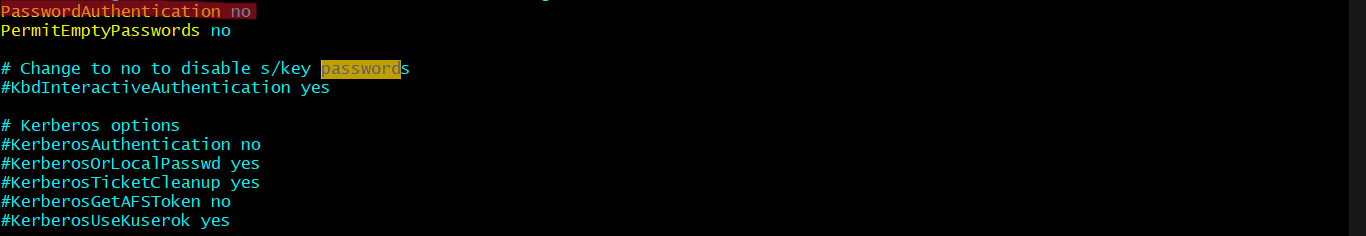
**Note:** If we want to assign users to primary group, we use **usermod -g <groupname> <username>** command&if wewant to assign users to secondary group, we use **usermod -aG <groupname> <username>** command,where **-a** denotes append.

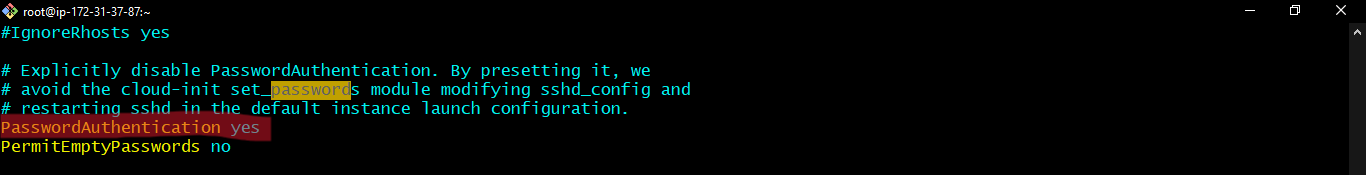
To check the group assign, we use the command **id <username>**

1. Now, we need to assign password to the users. **By default, Linux doesn’t support password-based authentication**.



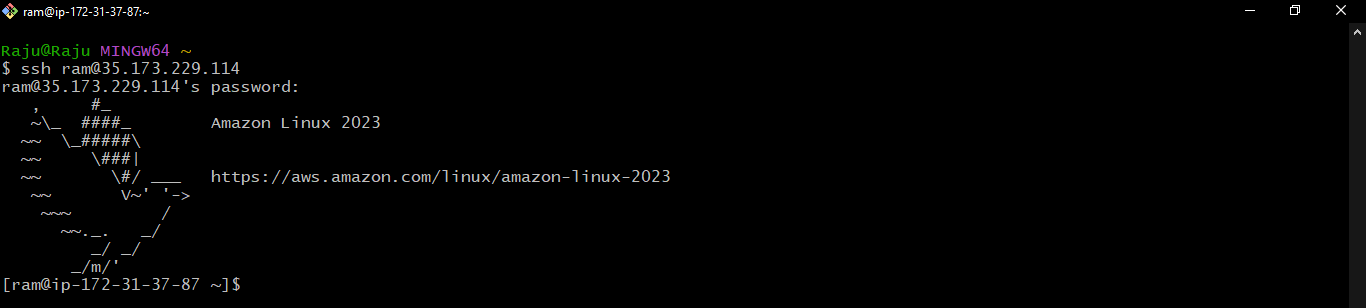
So, we need to make some changes in the **etc/ssh/sshd\_config** file. In this file, we need to search for password. There we can see **PasswordAuthentication no** and we need to change this to **PasswordAuthentication yes.**





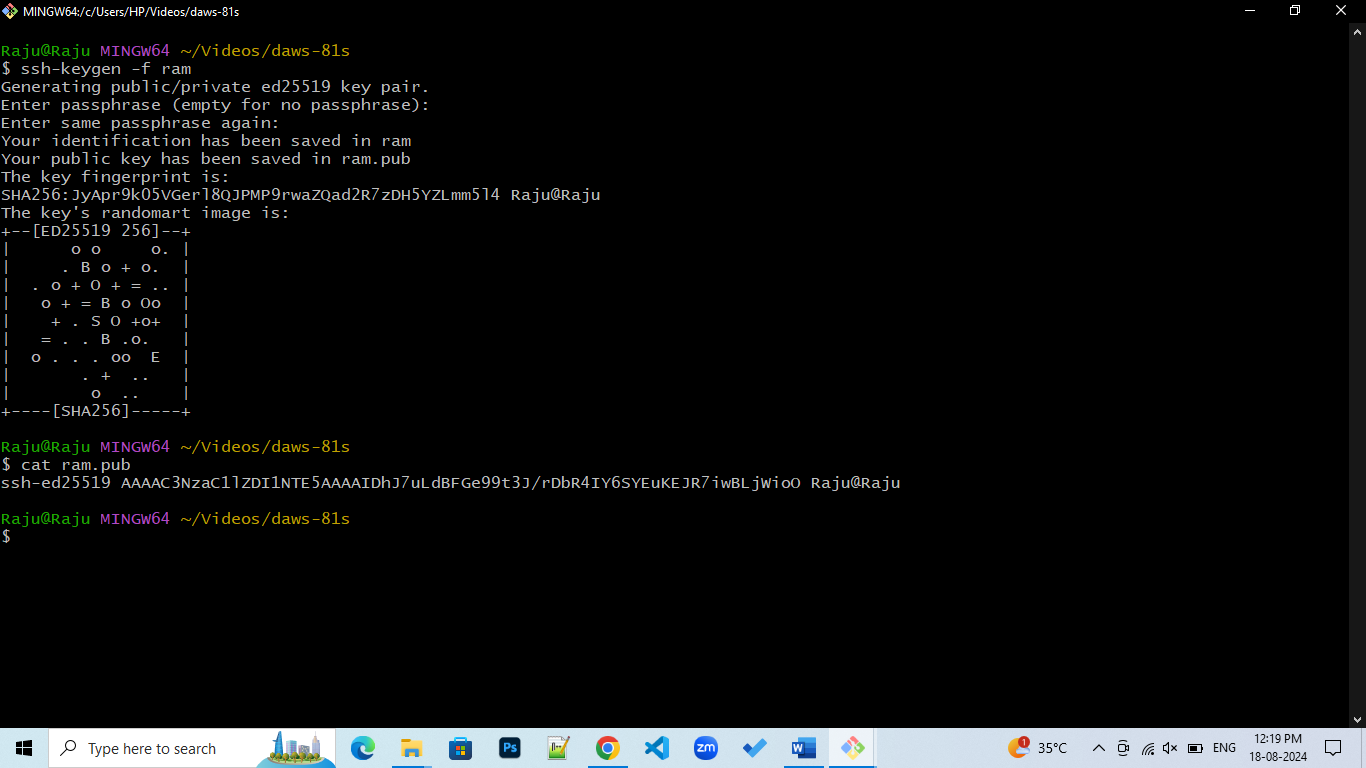
Then save the file and restart the **sshd** service using the command **systemctl restart sshd.**

1. Now open new terminal and login to **ram** user using password-based authentication through the following command **ssh username@IPAddress**

****

1. **Key-Based Authentication**

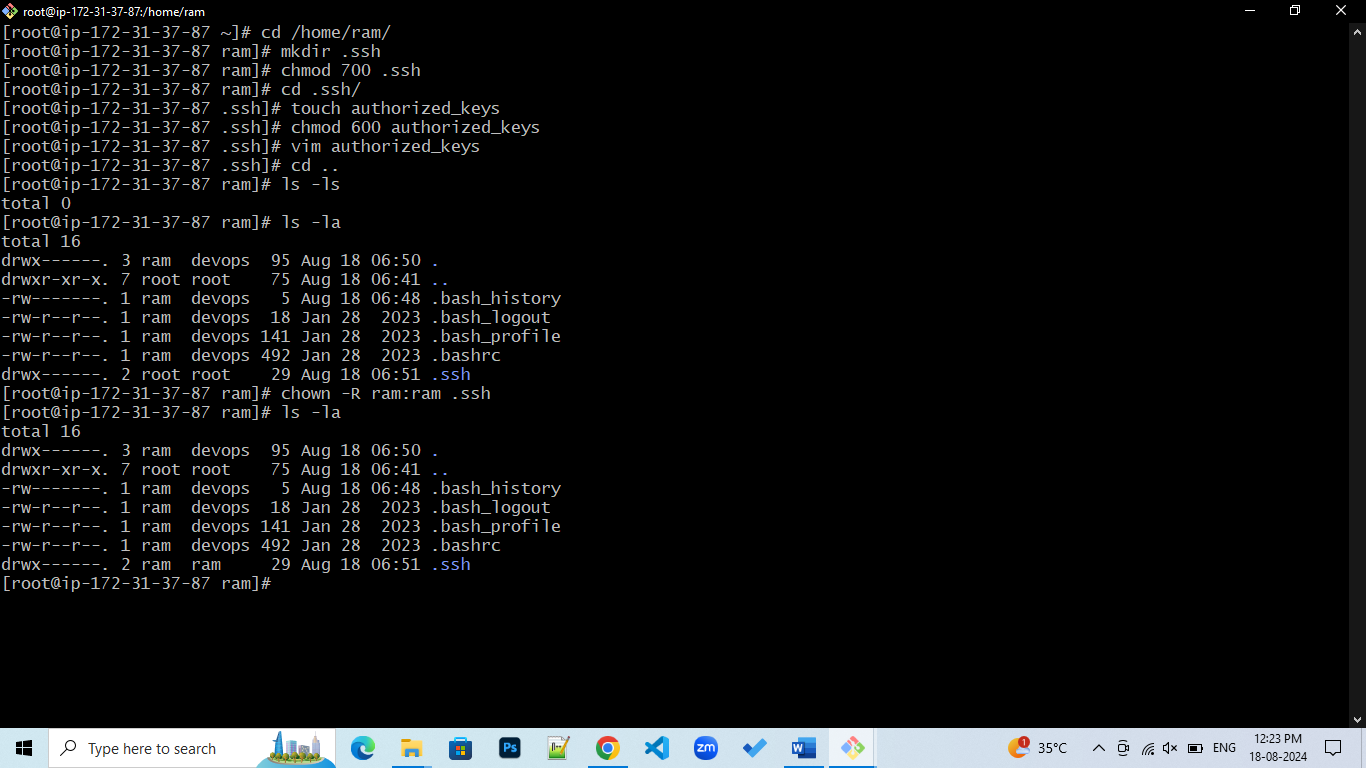
After successful login, we need to logout and need to generate ssh keys for the users in the local machine. We use the command **ssh-keygen -f <username>** for generating ssh keys.



Now login to ram user from root user and create .ssh folder in the home directory of the ram user. Then set the folder permission using **chmod 700 .ssh**

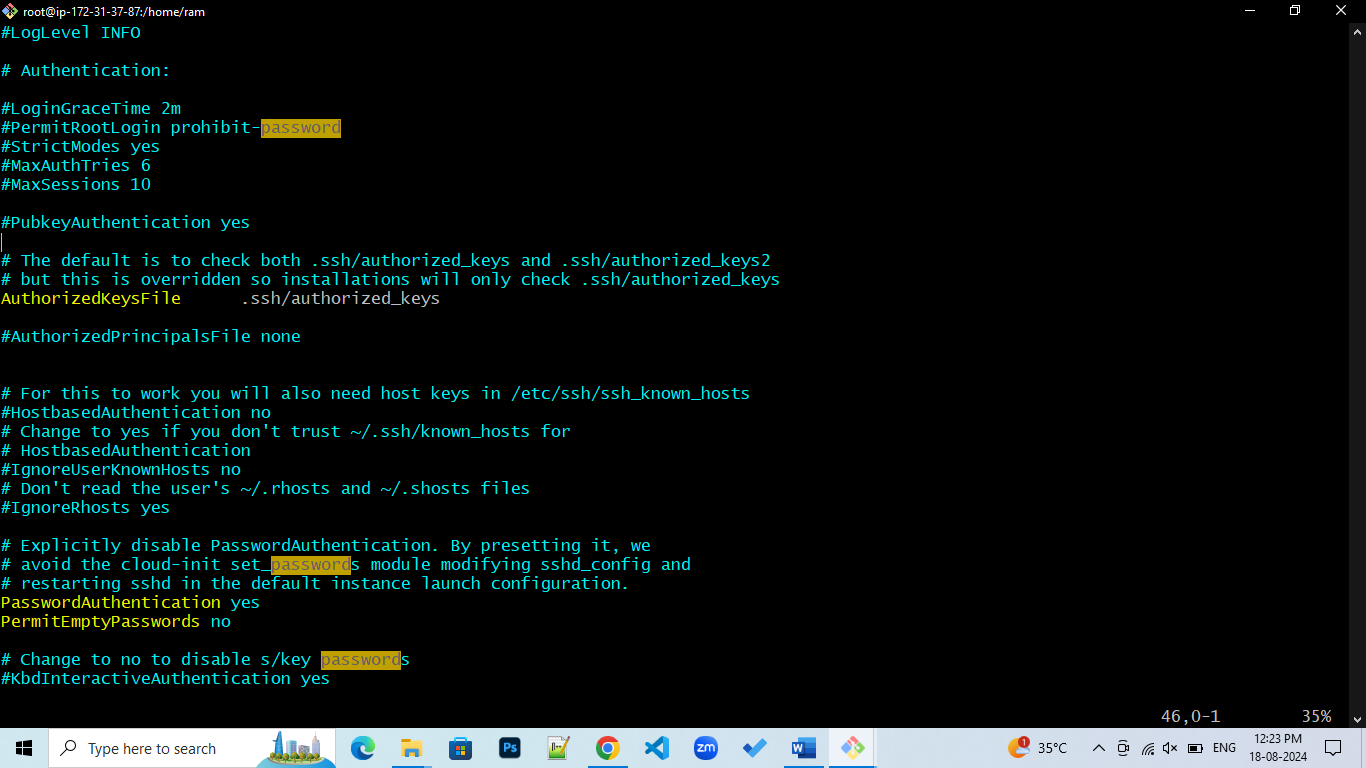
Then go inside the .ssh folder and create a file named authorized\_keys and set the file permissions using **chmod 600 authorized\_keys**

Copy the public key of ram user and paste in the authorized\_key file and save it. The owner of the .ssh file should be in the name of ram. **chown -R ram:ram .ssh**



1. **Disable Password-Based Authentication**

Now, we need to disable password-based authentication which we have enabled previously in the etc/sh/sshd\_config file and enable keybased authentication. Then restart the service.



1. **Testing & Verification**

Now go to the new terminal and login to ram user using key-based authentication and when we try to access through password-based authentication it will denies the request.

