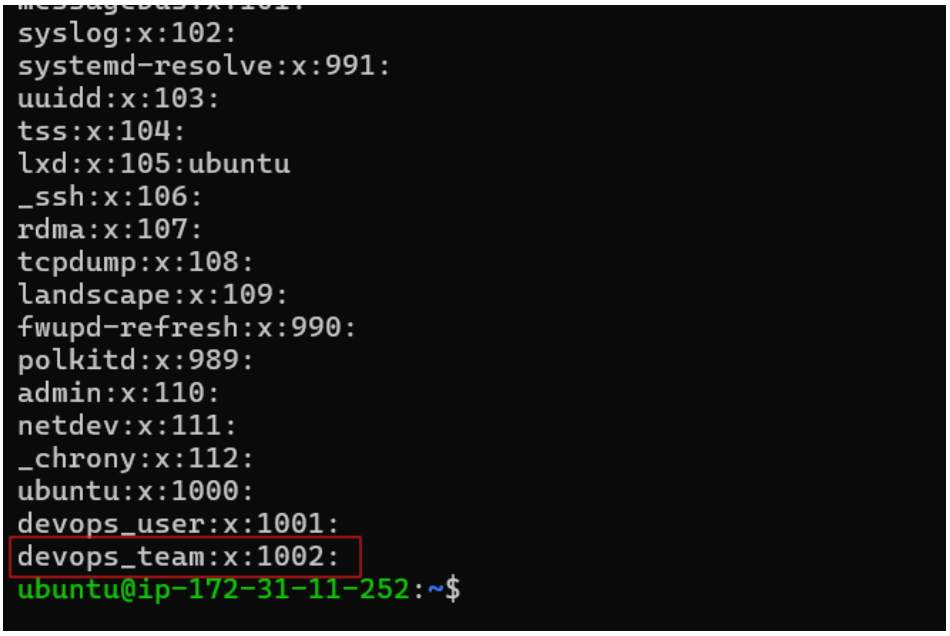
1️⃣ User & Group Management

Create a user devops_user and add them to a group devops_team.

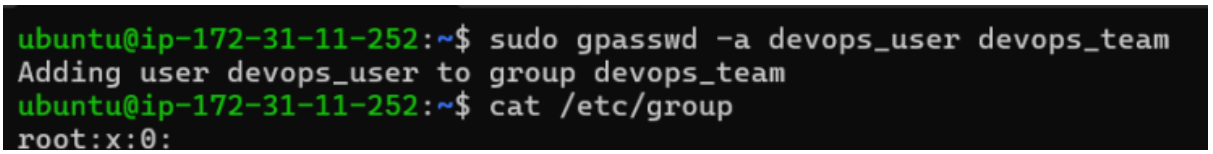
- To create the user in linux the command used is **sudo useradd -M devops_user**
- The users present in the system can be seen in the **/etc/passwd file**

```
ubuntu@ip-172-31-11-252:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uuidd:x:103:103::/run/uuidd:/usr/sbin/nologin
tss:x:104:104:TPM software stack,,,:/var/lib/tpm:/bin/false
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:106:1::/var/cache/pollinate:/bin/false
tcpdump:x:107:108::/nonexistent:/usr/sbin/nologin
landscape:x:108:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/:/usr/sbin/nologin
ec2-instance-connect:x:109:65534::/nonexistent:/usr/sbin/nologin
_chrony:x:110:112:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
devops_user:x:1001:1001::/home/devops_user:/bin/sh
```

- The list of the groups are present in /etc/group



- Now we need to add the devops_user to the group devops_team
- In order to do this we have a command : **sudo gpasswd -a devops_user devops_team**



Set a password and grant sudo access.

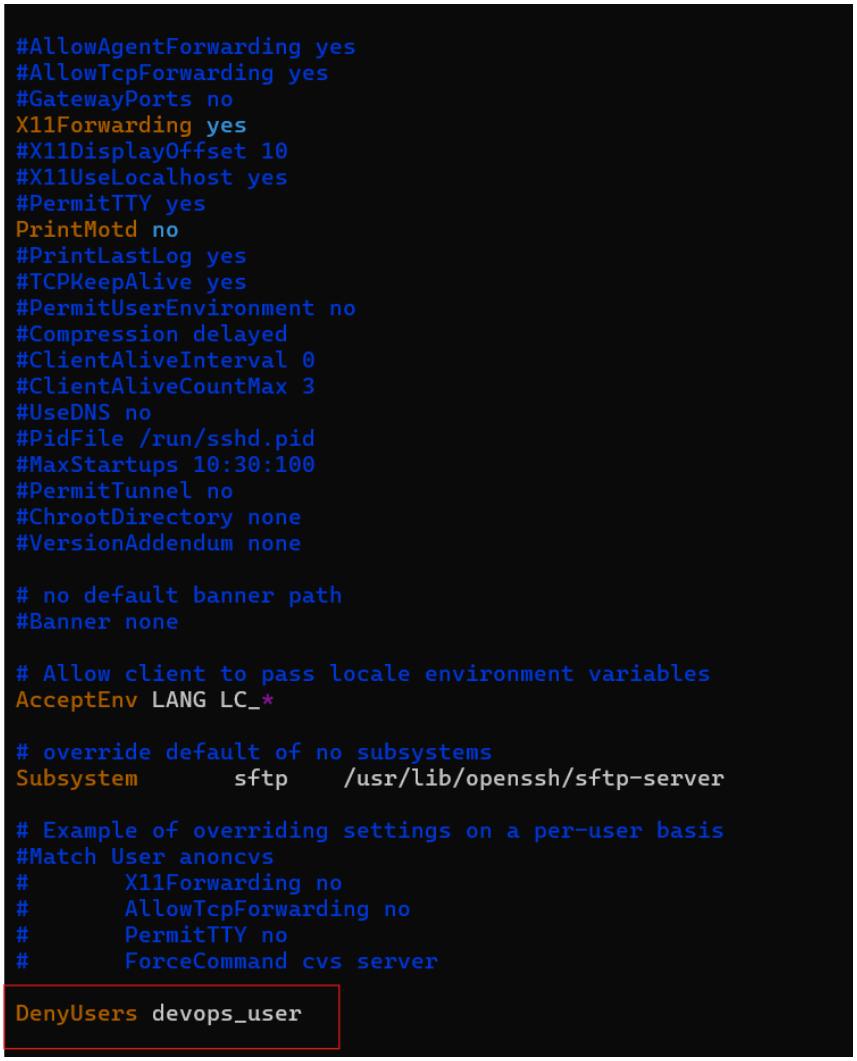
- In order to set the password and grant the user devops_user sudo access we need to add the user to the sudo group.
- This can be done using the command: **sudo usermod -aG sudo devops_user**

This shows that the user devops_user has been granted sudo permission

Restrict SSH login for certain users in /etc/ssh/sshd_config.

- To deny the ssh login to the user we need to append DenyUsers <theusername> to the file **/etc/ssh/sshd_config**

- Adding the DenyUser devops_user command to the file



2 File & Directory Permissions

- **Create /devops_workspace and a file project_notes.txt.**

    - To create the directory devops_workspace : **mkdir devops_workspace**
    - Change the directory to devops_workspace: **cd devops_workspace**
    - Create a file project_notes.txt : **touch project_notes.txt.**

```
ubuntu@ip-172-31-11-252:~$ mkdir devops_workspace
ubuntu@ip-172-31-11-252:~$ cd devops_workspace/
ubuntu@ip-172-31-11-252:~/devops_workspace$ touch project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$ ls -l
total 0
-rw-rw-r-- 1 ubuntu ubuntu 0 Feb  9 14:03 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

- **Set permissions:Owner can edit, group can read, others have no access. Use ls -l to verify permissions.**

    - Check the initial permission of the file project_notes.txt using **ls -l command.** The below screenshot shows that the user and group has read and write access but other users have read only access

```
ubuntu@ip-172-31-11-252:~$ cd  devops_workspace/
ubuntu@ip-172-31-11-252:~/devops_workspace$ ls -l
total 0
-rw-rw-r-- 1 ubuntu ubuntu 0 Feb  9 14:03 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

    - Permission is set using the chmod command, where the owner can edit, group can read and others have no access

      Command: chmod 640 project_notes.txt

```
ubuntu@ip-172-31-11-252:~/devops_workspace$ chmod 640 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$ ls -l
total 0
-rw-r----- 1 ubuntu ubuntu 0 Feb  9 14:03 project_notes.txt
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

3️⃣Log File Analysis with AWK, Grep & Sed

- Download the log file from the repository Linux_2k.log
- Command : curl -O https://github.com/logpai/loghub/blob/master/Linux/Linux_2k.log

```
ubuntu@ip-172-31-11-252:~/devops_workspace$ curl -O https://github.com/logpai/loghub/blob/master/Linux/Linux_2k.log
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  876k    0  876k    0     0  1177k      0 --:--:-- --:--:-- --:--:-- 1177k
ubuntu@ip-172-31-11-252:~/devops_workspace$
```

- Extract insights using commands:
- Use grep to find all occurrences of the word "error".