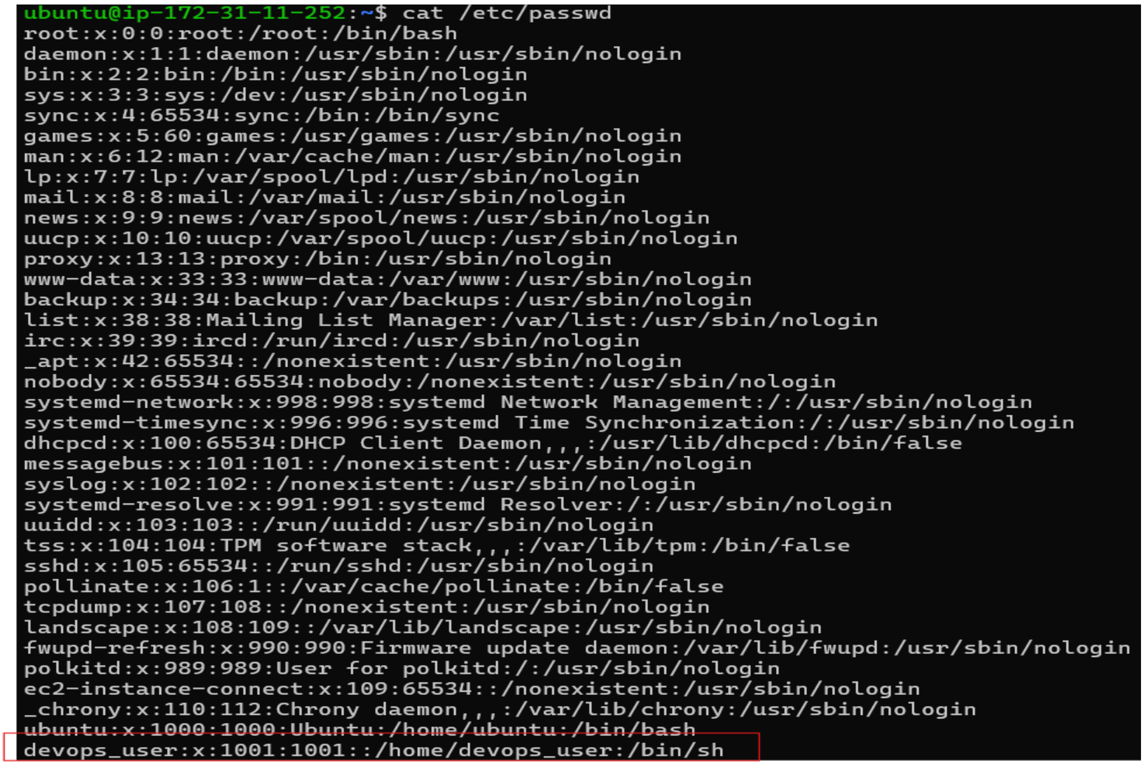
1️⃣User & Group Management

Task:

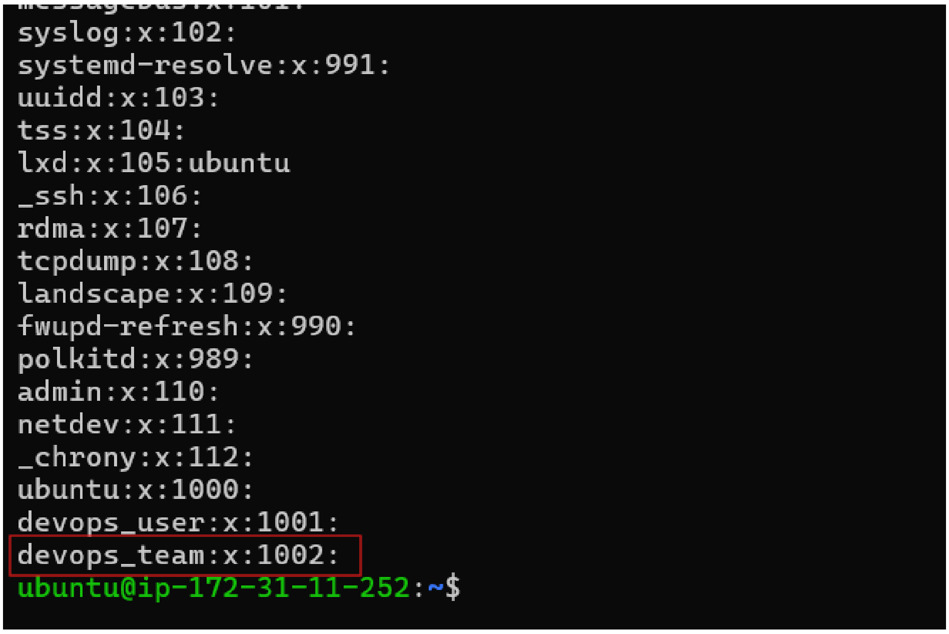
Create a user devops_user and add them to a group devops_team.

- 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
```

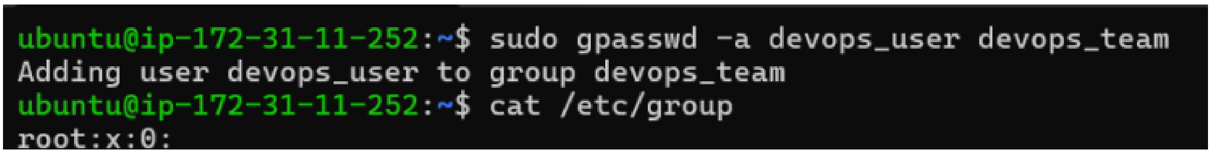
- The list of the groups are present in /etc/group



```
messagebus:x:101:
syslog:x:102:
systemd-resolve:x:991:
uuidd:x:103:
tss:x:104:
lxd:x:105:ubuntu
_ssh:x:106:
rdma:x:107:
tcpdump:x:108:
landscape:x:109:
fwupd-refresh:x:990:
polkitd:x:989:
admin:x:110:
netdev:x:111:
_chrony:x:112:
ubuntu:x:1000:
devops_user:x:1001:
devops_team:x:1002:
ubuntu@ip-172-31-11-252:~$
```

- 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**

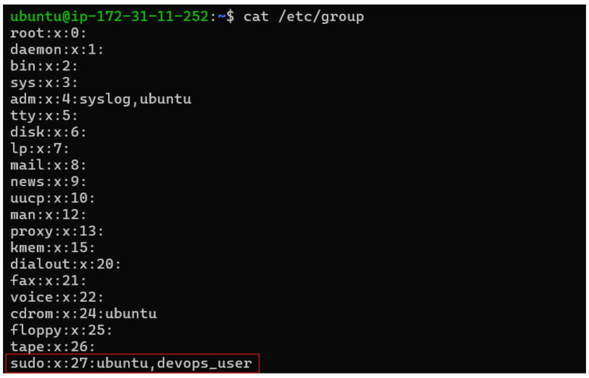


```
ubuntu@ip-172-31-11-252:~$ sudo gpasswd -a devops_user devops_team
Adding user devops_user to group devops_team
ubuntu@ip-172-31-11-252:~$ cat /etc/group
root:x:0:
```

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**



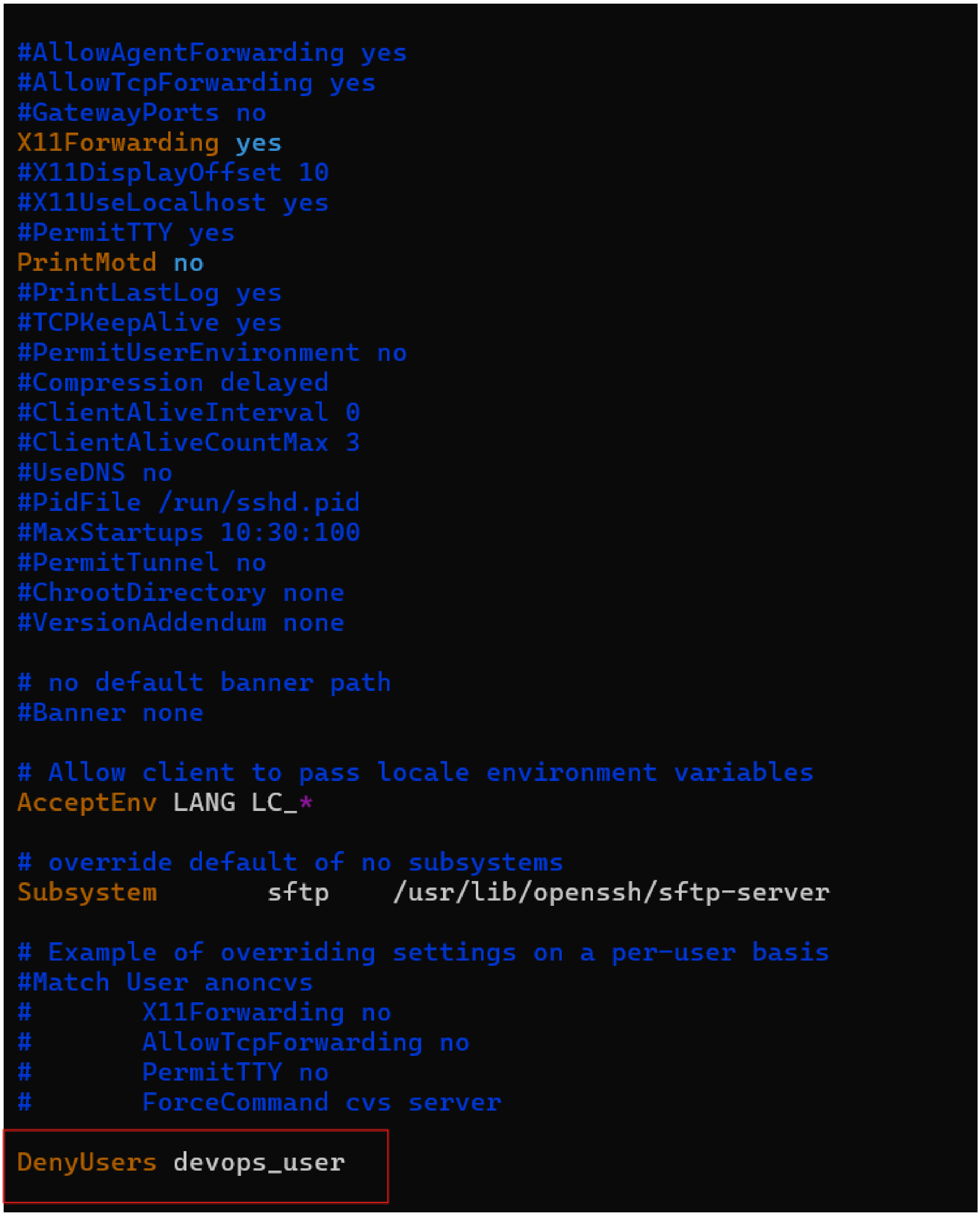
```
ubuntu@ip-172-31-11-252:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:ubuntu
floppy:x:25:
tape:x:26:
sudo:x:27:ubuntu,devops_user
```

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



```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

DenyUsers devops_user
```