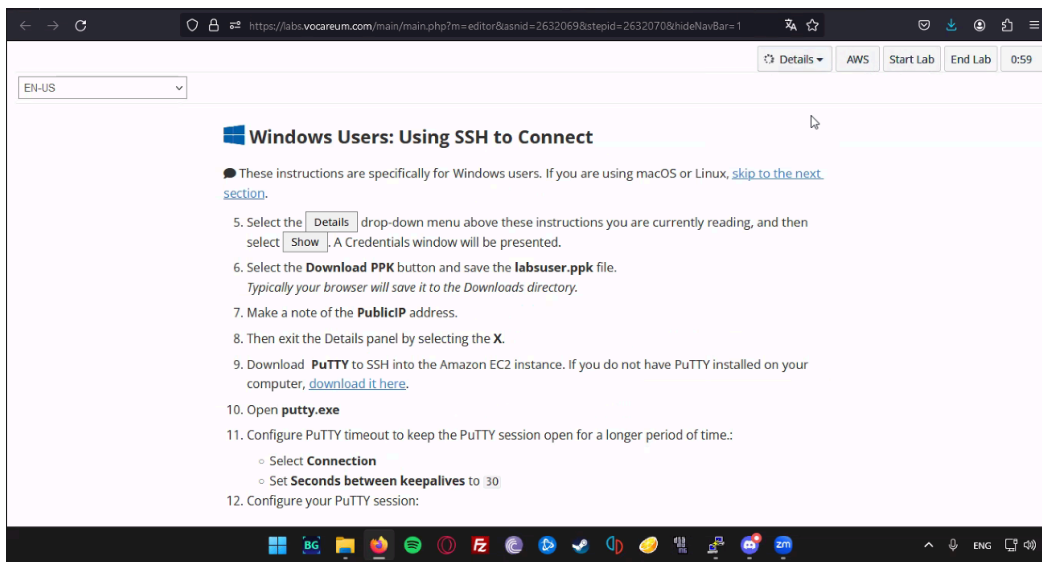


Lab 229 LX Usuarios y grupos

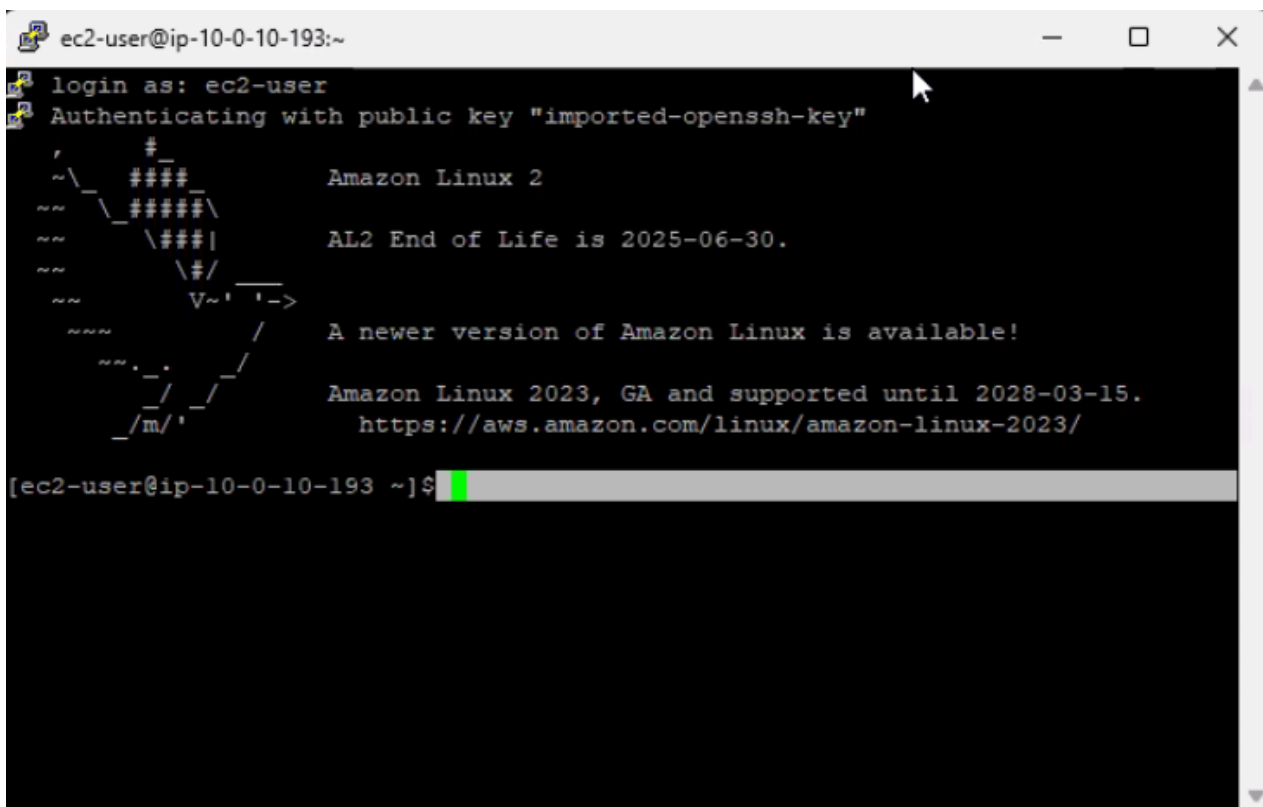
Grupo: Sony Etcheverry , Benjamin Sabaño, Micaela Viazzi, Fernanda Tatiana Rosa, Manuela Rodríguez

Primero iniciamos el Lab, haciendo click en el Start Lab.



Para ver cómo iniciamos la consola en más detalle, citamos el lab de Sony: [Lab](#)

Una vez que iniciamos la consola de Linux:



Hacemos PWD para comprobar que estamos en la carpeta correcta.

Usamos Sudo para obtener super permisos. Sin esto, aunque utilicemos useradd, no funcionará el comando.

Luego creamos los usuarios y se les asigna a cada uno la contraseña.

```
ec2-user@ip-10-0-10-193:~  
~~~~  
A newer version of Amazon Linux is available!  
~~~~  
Amazon Linux 2023, GA and supported until 2028-03-15.  
https://aws.amazon.com/linux/amazon-linux-2023/  
~~~~  
[ec2-user@ip-10-0-10-193 ~]$ pws  
-bash: pws: command not found  
[ec2-user@ip-10-0-10-193 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-10-0-10-193 ~]$ sudo useradd arosalez  
useradd: user 'arosalez' already exists  
[ec2-user@ip-10-0-10-193 ~]$ sudo userdelete arosalez  
sudo: userdelete: command not found  
[ec2-user@ip-10-0-10-193 ~]$ sudo userdel arosalez  
[ec2-user@ip-10-0-10-193 ~]$ sudo useradd arosalez  
useradd: warning: the home directory already exists.  
Not copying any file from skel directory into it.  
Creating mailbox file: File exists  
[ec2-user@ip-10-0-10-193 ~]$ sudo passwd arosalez  
Changing password for user arosalez.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-10-0-10-193 ~]$
```

Aquí comprobamos que creamos nuestro primer usuario utilizando `sudo cat /etc/passwd | cut -d: -f1`.

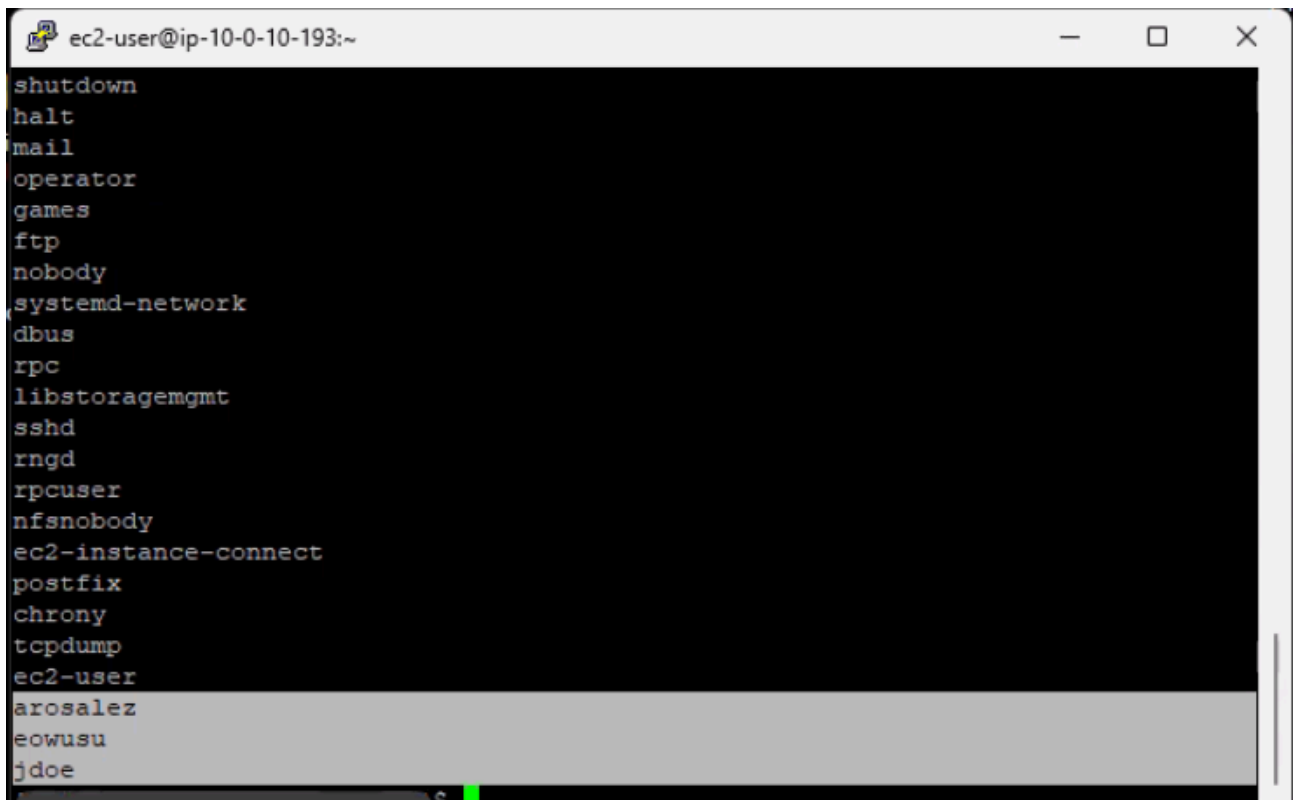
```
ec2-user  
arosalez  
[ec2-user@ip-10-0-10-193 ~]$
```

Una vez que añadimos nuestro primer usuario, añadimos dos más: eowusu y jdoe.

```
sudo useradd eowusu  
sudo useradd jdoe
```

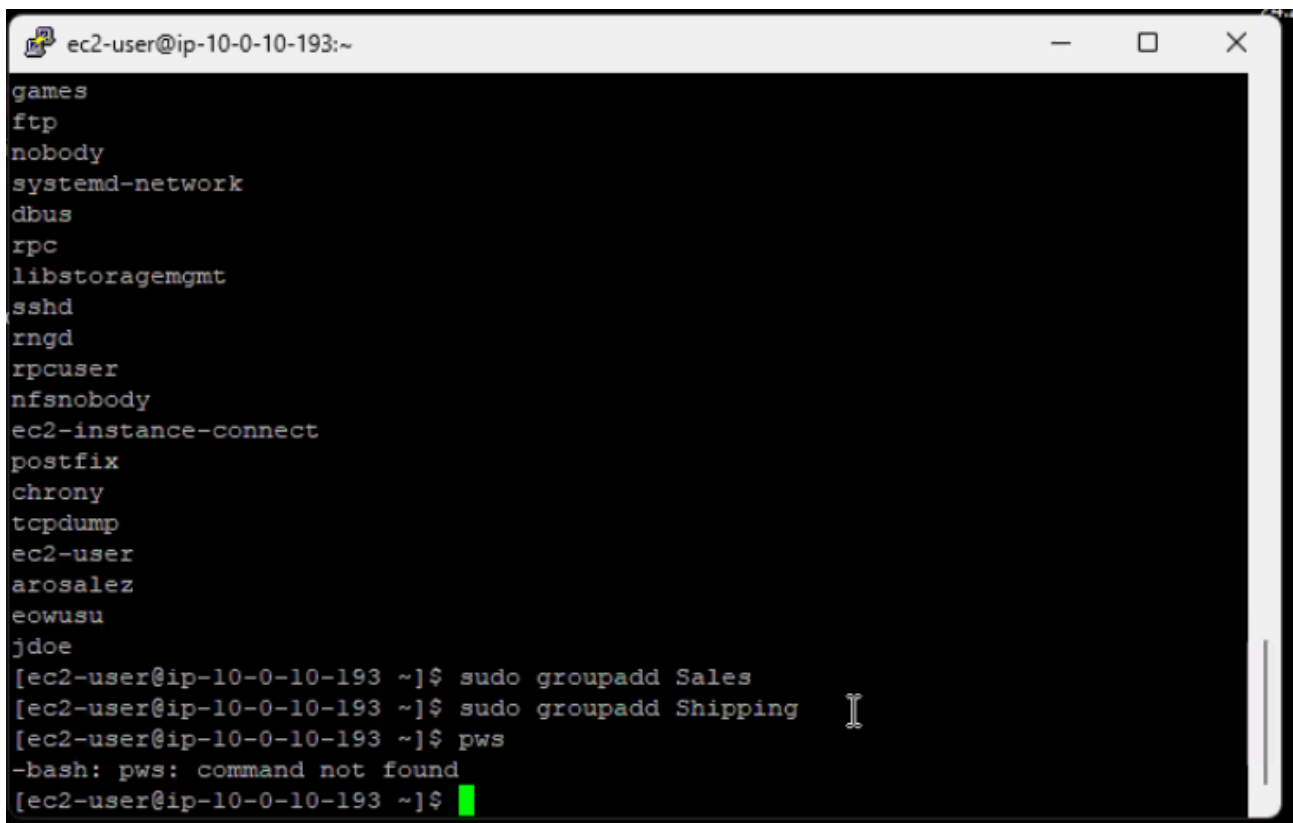
```
ec2-user@ip-10-0-10-193:~  
games  
ftp  
nobody  
systemd-network  
dbus  
rpc  
libstoragemgmt  
sshd  
rngd  
rpcuser  
nfsnobody  
ec2-instance-connect  
postfix  
chrony  
tcpdump  
ec2-user  
arosalez  
[ec2-user@ip-10-0-10-193 ~]$ sudo useradd eowusu  
[ec2-user@ip-10-0-10-193 ~]$ sudo passwd eowusu  
Changing password for user eowusu.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[ec2-user@ip-10-0-10-193 ~]$
```

Aquí podemos ver los 3 usuarios ya creados, volviendo a utilizar el comando `sudo cat /etc/passwd | cut -d: -f1`.



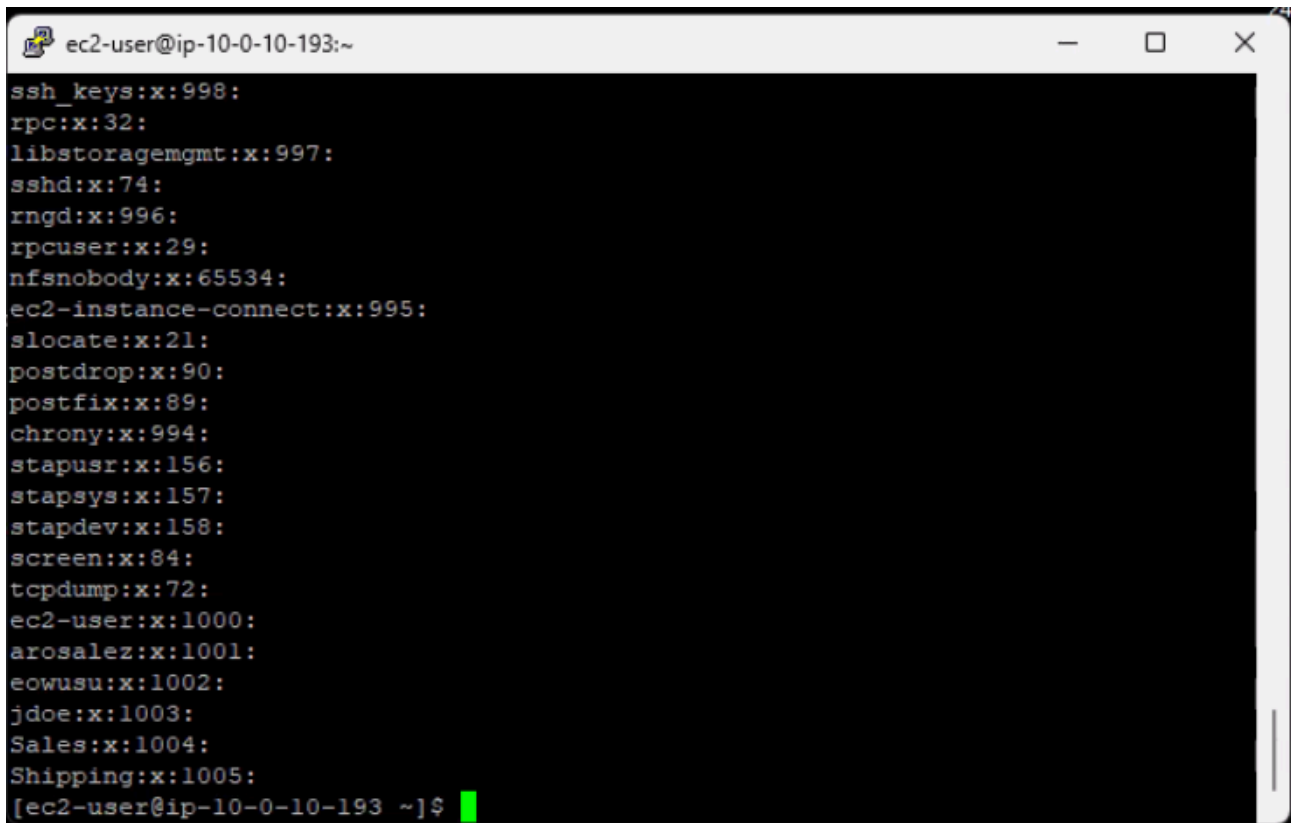
```
ec2-user@ip-10-0-10-193:~  
shutdown  
halt  
mail  
operator  
games  
ftp  
nobody  
systemd-network  
dbus  
rpc  
libstoragemgmt  
sshd  
rngd  
rpcuser  
nfsnobody  
ec2-instance-connect  
postfix  
chrony  
tcpdump  
ec2-user  
arosalez  
eowusu  
jdoe
```

Creamos los grupos Sales y Shipping `sudo groupadd Sales`.



```
ec2-user@ip-10-0-10-193:~  
games  
ftp  
nobody  
systemd-network  
dbus  
rpc  
libstoragemgmt  
sshd  
rngd  
rpcuser  
nfsnobody  
ec2-instance-connect  
postfix  
chrony  
tcpdump  
ec2-user  
arosalez  
eowusu  
jdoe  
[ec2-user@ip-10-0-10-193 ~]$ sudo groupadd Sales  
[ec2-user@ip-10-0-10-193 ~]$ sudo groupadd Shipping  
[ec2-user@ip-10-0-10-193 ~]$ pws  
-bash: pws: command not found  
[ec2-user@ip-10-0-10-193 ~]$
```

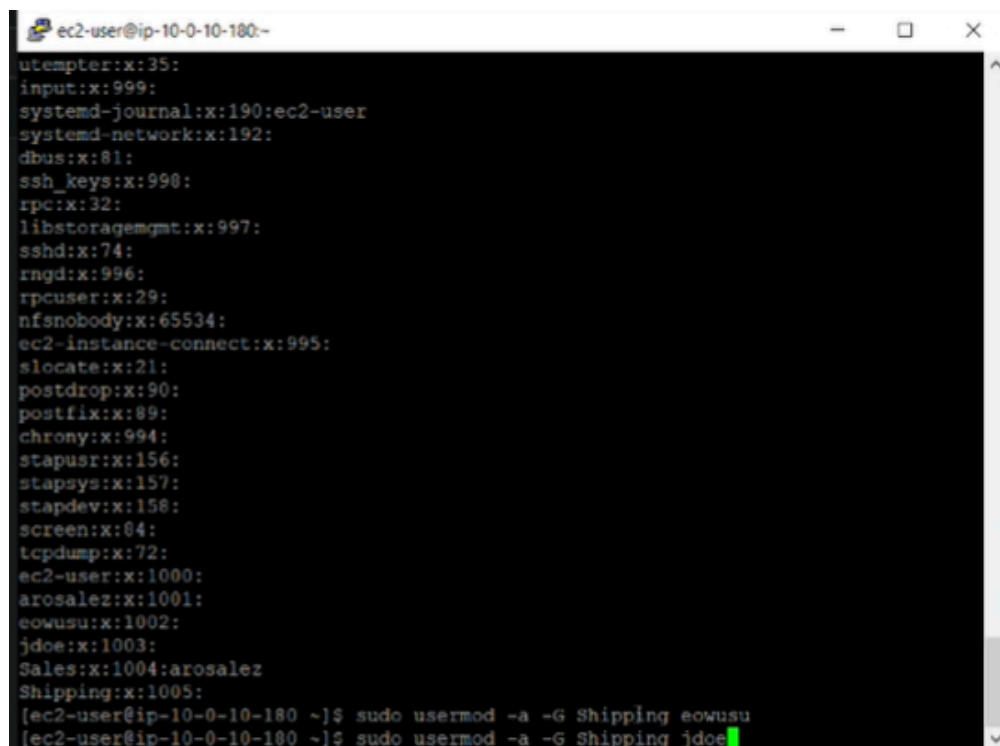
Comprobamos que se hayan añadido. Utilizando nuevamente el comando `sudo cat /etc/passwd | cut -d: -f1`.



```
ec2-user@ip-10-0-10-193:~  
ssh_keys:x:998:  
rpc:x:32:  
libstoragemgmt:x:997:  
sshd:x:74:  
rngd:x:996:  
rpcuser:x:29:  
nfsnobody:x:65534:  
ec2-instance-connect:x:995:  
slocate:x:21:  
postdrop:x:90:  
postfix:x:89:  
chrony:x:994:  
stapusr:x:156:  
stapusr:x:157:  
stapdev:x:158:  
screen:x:84:  
tcpdump:x:72:  
ec2-user:x:1000:  
arosalez:x:1001:  
eowusu:x:1002:  
jdoe:x:1003:  
Sales:x:1004:  
Shipping:x:1005:  
[ec2-user@ip-10-0-10-193 ~]$
```

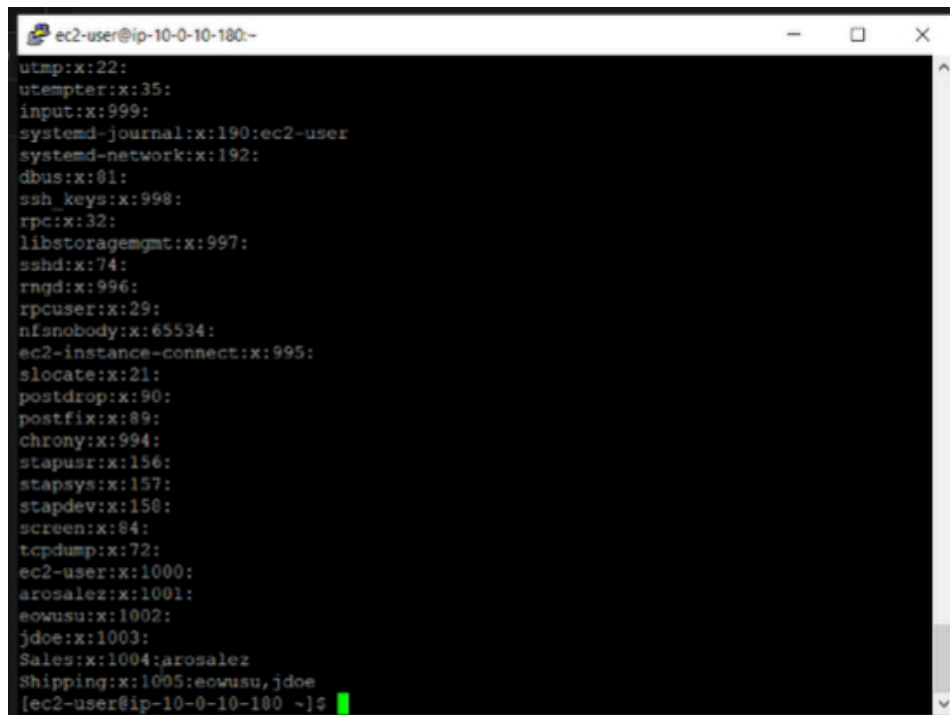
Para añadir a los usuarios a los grupos, primero hacemos una prueba, añadiendo primero al usuario arosalez al grupo Sales.

`sudo usermod -a -G Sales arosalez`



```
ec2-user@ip-10-0-10-180:~  
utempter:x:35:  
input:x:999:  
systemd-journal:x:190:ec2-user  
systemd-network:x:192:  
dbus:x:81:  
ssh_keys:x:990:  
rpc:x:32:  
libstoragemgmt:x:997:  
sshd:x:74:  
rngd:x:996:  
rpcuser:x:29:  
nfsnobody:x:65534:  
ec2-instance-connect:x:995:  
slocate:x:21:  
postdrop:x:90:  
postfix:x:89:  
chrony:x:994:  
stapusr:x:156:  
stapusr:x:157:  
stapdev:x:158:  
screen:x:84:  
tcpdump:x:72:  
ec2-user:x:1000:  
arosalez:x:1001:  
eowusu:x:1002:  
jdoe:x:1003:  
Sales:x:1004:arosalez  
Shipping:x:1005:  
[ec2-user@ip-10-0-10-180 ~]$ sudo usermod -a -G Shipping eowusu  
[ec2-user@ip-10-0-10-180 ~]$ sudo usermod -a -G Shipping jdoe
```

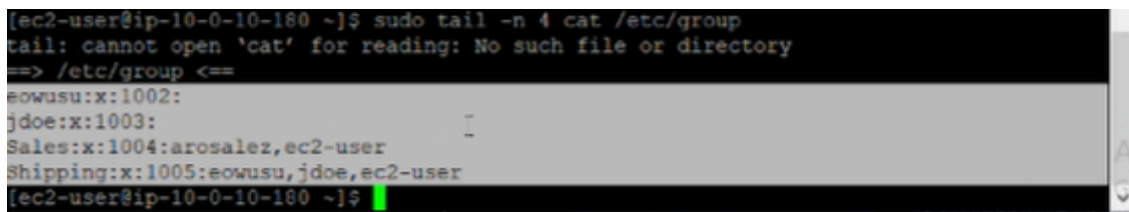
Visualizamos los usuarios en los grupos, nuevamente con el comando `sudo cat /etc/passwd | cut -d: -f1.`

A terminal window titled 'ec2-user@ip-10-0-10-180-' showing the output of the command 'sudo cat /etc/passwd | cut -d: -f1'. The output lists system users and regular users, including 'ec2-user' which is part of the 'ec2-user' group.

```
utmp:x:22:
utempter:x:35:
input:x:999:
systemd-journal:x:190:ec2-user
systemd-network:x:192:
dbus:x:81:
ssh_keys:x:998:
rpc:x:32:
libstoragemgmt:x:997:
sshd:x:74:
rngd:x:996:
rpcuser:x:29:
nfsnobody:x:65534:
ec2-instance-connect:x:995:
slocate:x:21:
postdrop:x:90:
postfix:x:89:
chrony:x:994:
stapusr:x:156:
stapusr:x:157:
stapdev:x:156:
screen:x:84:
tcpdump:x:72:
ec2-user:x:1000:
arosalez:x:1001:
eowusu:x:1002:
jdoe:x:1003:
Sales:x:1004:arosalez
Shipping:x:1005:eowusu,jdoe
[ec2-user@ip-10-0-10-180 ~]$
```

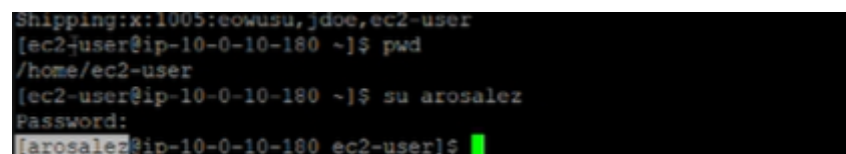
Aquí mostramos que agregamos ec2-user en los grupos anteriores. Para agregar ec2-user usamos

`sudo usermod -a -G (Grupo Correspondiente) ec2-user`

A terminal window showing the output of the command 'sudo tail -n 4 cat /etc/group'. The output shows the last four lines of the /etc/group file, including 'ec2-user' as a member of the 'Sales' and 'Shipping' groups.

```
[ec2-user@ip-10-0-10-180 ~]$ sudo tail -n 4 cat /etc/group
tail: cannot open 'cat' for reading: No such file or directory
==> /etc/group <==
eowusu:x:1002:
jdoe:x:1003:
Sales:x:1004:arosalez,ec2-user
Shipping:x:1005:eowusu,jdoe,ec2-user
[ec2-user@ip-10-0-10-180 ~]$
```

Iniciamos sesión con el usuario, con el comando: `su arosalez`

A terminal window showing the command 'su arosalez' being executed. The prompt changes from '[ec2-user@ip-10-0-10-180 ~]\$' to '[arosalez@ip-10-0-10-180 ec2-user]\$', indicating a successful switch to the 'arosalez' user.

```
Shipping:x:1005:eowusu,jdoe,ec2-user
[ec2-user@ip-10-0-10-180 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-180 ~]$ su arosalez
Password:
[arosalez@ip-10-0-10-180 ec2-user]$
```

Observamos que el usuario no tiene permisos cuando intentamos hacer `touch myFile.txt.`

```
ec2-user@ip-10-0-10-180:~  
[arosalez@ip-10-0-10-180 ec2-user]$ touch myFile.txt  
touch: cannot touch 'myFile.txt': Permission denied  
[arosalez@ip-10-0-10-180 ec2-user]$ sudo touch myFile.txt  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for arosalez:  
arosalez is not in the sudoers file. This incident will be reported.  
[arosalez@ip-10-0-10-180 ec2-user]$ exit  
exit  
[ec2-user@ip-10-0-10-180 ~]$
```

Ahora observamos el contenido del archivo, examinamos el contenido seguro y podemos ver que se realizó una acción no permitida. Nos muestra que 'arosalez' no está incluido en sudoers, por lo tanto, no nos permite realizar ninguna acción.

```
sudo cat /var/log/secure
```

```
2-user(uid=1000)  
Apr 20 17:31:41 ip-10-0-10-180 sudo: arosalez : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/ec2  
-user ; USER=root ; COMMAND=/bin/touch#040myFile.txt  
Apr 20 17:32:19 ip-10-0-10-180 su: pam_unix(su:session): session closed for user arosalez
```