



| Lab 229

Users and Groups

Student: Mane Zakarian

Bootcamp: Forge AWS re/Start UYMON5

Date: 2023



Objectives

In this lab, you will:

- Create new users with a default password
- Create groups and assign the appropriate users
- Log in as different users

Accessing the AWS Management Console

1. At the top of these instructions, choose **Start Lab** to launch your lab. A **Start Lab** panel opens, and it displays the lab status.

Tip: If you need more time to complete the lab, choose the Start Lab button again to restart the timer for the environment.

2. Wait until you see the message *Lab status: ready*, then close the **Start Lab** panel by choosing the X.
3. At the top of these instructions, choose **AWS**. This opens the AWS Management Console in a new browser tab. The system will automatically log you in.

Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with a message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon and then choose **Allow pop ups**.

4. Arrange the AWS Management Console tab so that it displays alongside these instructions. Ideally, you will be able to see both browser tabs at the same time so that you can follow the lab steps more easily.

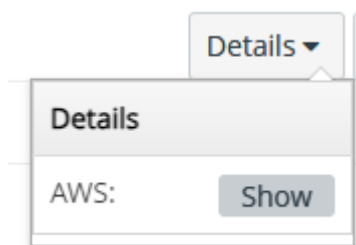


Task 1: Use SSH to connect to an Amazon Linux EC2 instance

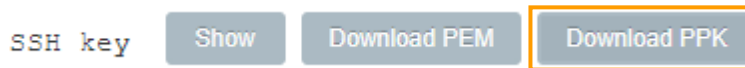
In this task, you will connect to a Amazon Linux EC2 instance. You will use an SSH utility to perform all of these operations.

Windows Users: Using SSH to Connect

1. Select the `Details` drop-down menu above these instructions you are currently reading, and then select `Show`. A Credentials window will be presented.



2. Select the **Download PPK** button and save the `labsuser.ppk` file.



3. Make a note of the **PublicIP** address.

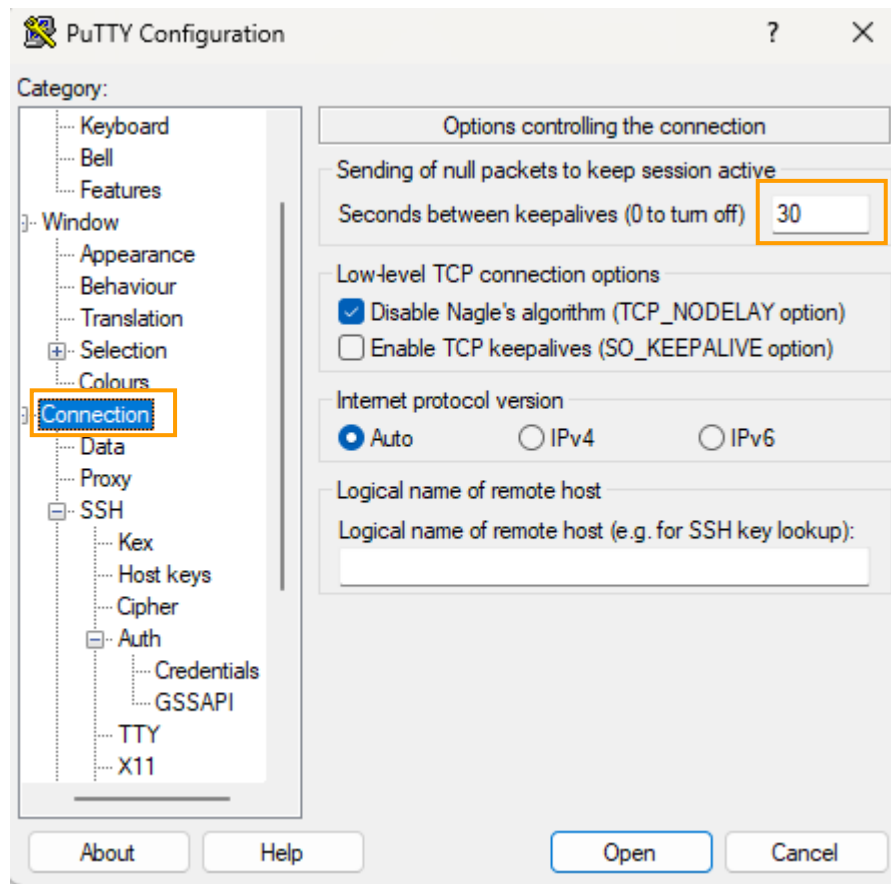
`PublicIP`

`52.34.82.18`

4. Then exit the Details panel by selecting the X.
5. Download **PuTTY** to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer.
6. Open **putty.exe**
7. Configure PuTTY timeout to keep the PuTTY session open for a longer period of time.:



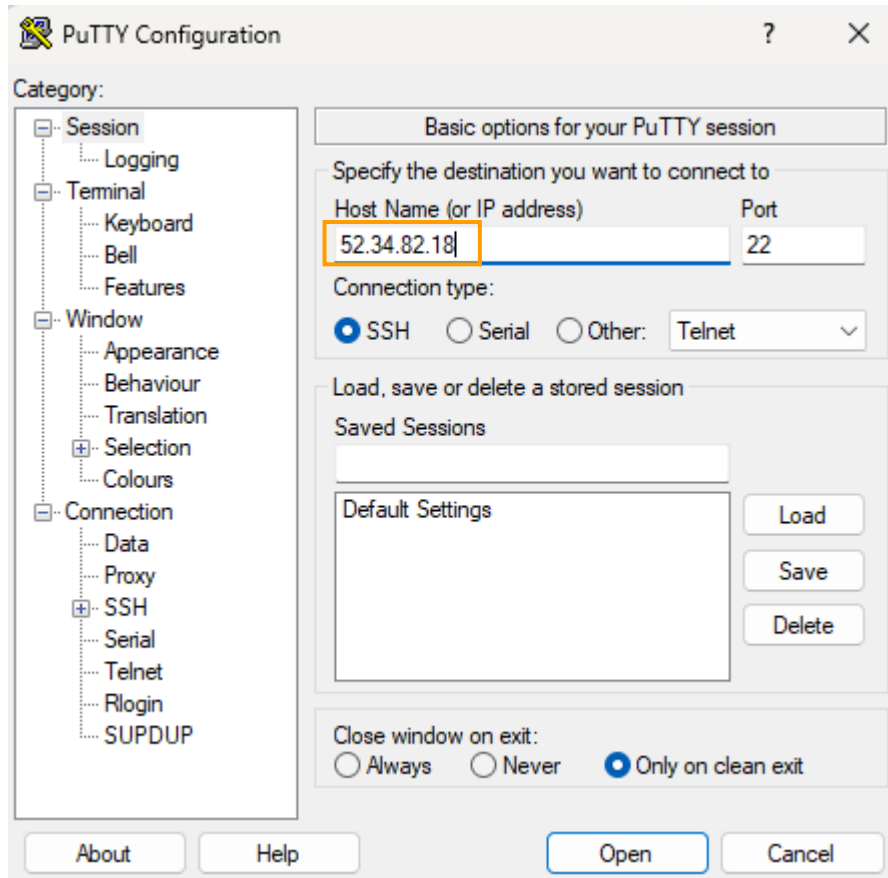
- Select **Connection**
- Set **Seconds between keepalives** to **30**



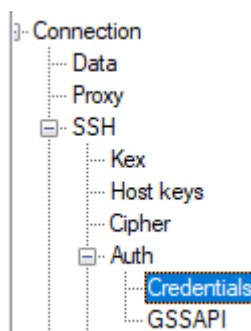
8. Configure your PuTTY session:
- Select **Session**



- **Host Name (or IP address):** Paste the **Public DNS or IPv4 address** of the instance you made a note of earlier. Alternatively, return to the EC2 Console and select **Instances**. Check the box next to the instance you want to connect to and in the *Description* tab copy the **IPv4 Public IP** value

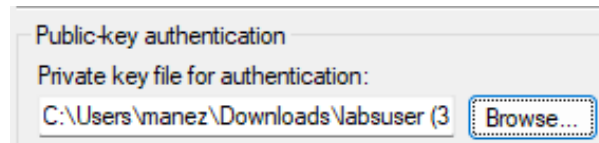


- Back in PuTTY, in the **Connection** list, expand **SSH** and select **Auth** (*don't expand it*)

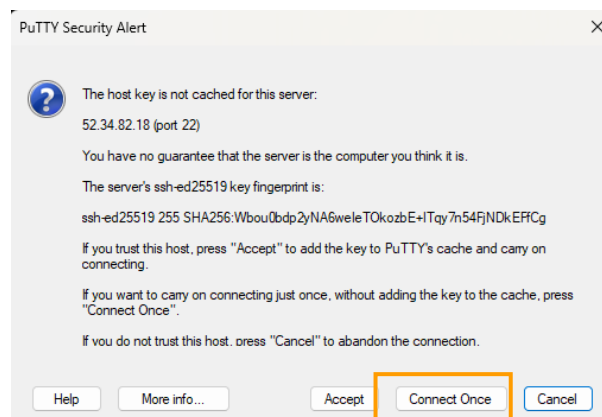




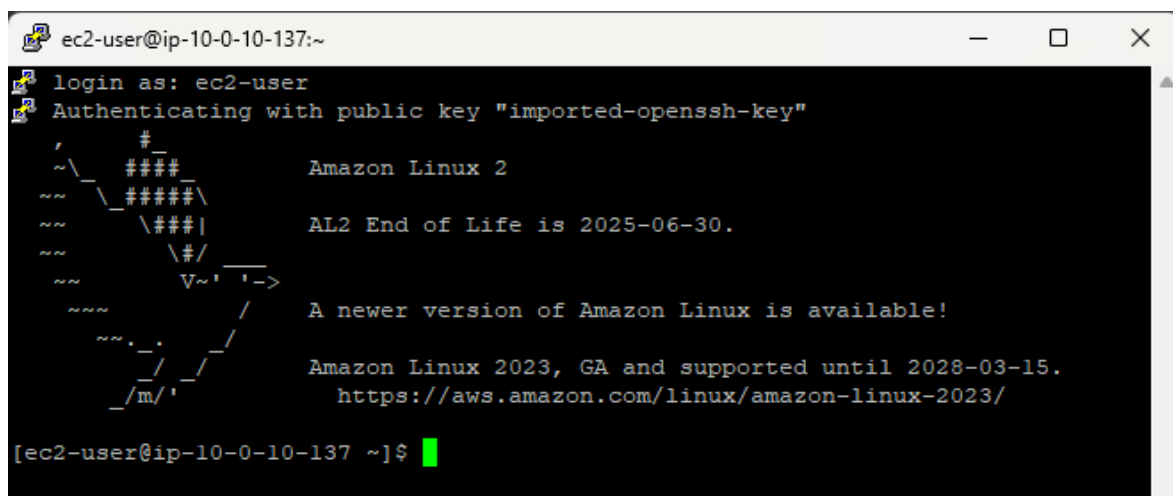
- Select **Browse** and select the lab#.ppk file that you downloaded



- Select **Open** to select it and then select **Open** again.
9. Select **Yes**, to trust and connect to the host.



10. When prompted **login as**, enter: `ec2-user` This will connect you to the EC2 instance.





Task 2: Create Users

In this section, you create users based on the following table:

First Name	Surname	Job Role	Starting Password
Mane	Zakarian	Sales	Hello1234
Andres	Colazabal	HR	Hello1234
Catalina	Puñales	Personnel	Hello1234
Emiliano	Corbalan	Finance	Hello1234

Ensure that you are spelling the user IDs correctly so that these users can use default credentials to log in.

24. Validate that you are in the home folder of your current user by typing **pwd** and pressing ENTER.

```
[ec2-user]$ pwd
/home/ec2-user
[ec2-user]$
```

```
[ec2-user@ip-10-0-10-122 ~]$ pwd
/home/ec2-user
```

25. To add the users from the list above, enter `sudo useradd mane` / `sudo useradd emiliano` / `sudo useradd catalina` / `sudo useradd andres` and press Enter. This step creates the users.

```
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd mane
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd emiliano
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd catalina
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd andres
[ec2-user@ip-10-0-10-122 ~]$
```

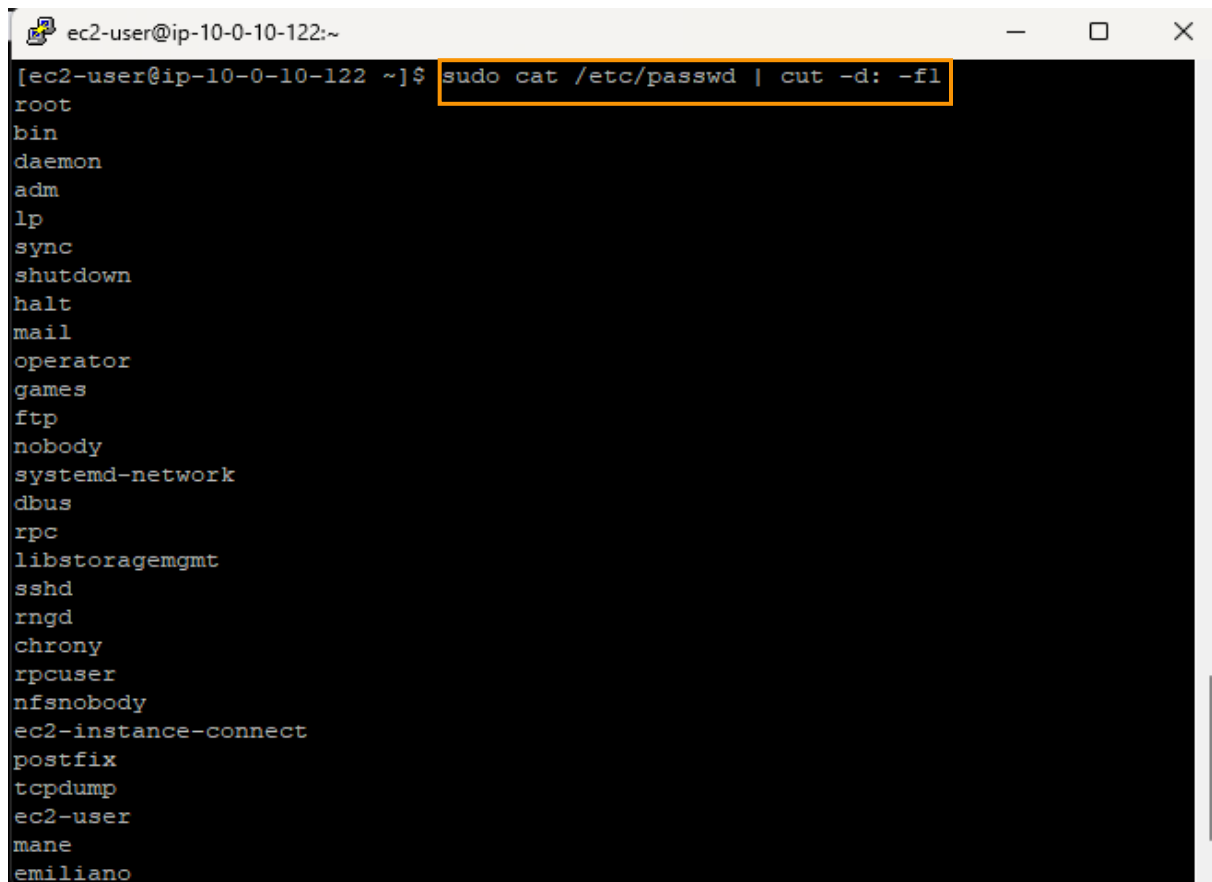


26. Enter `sudo passwd useradd mane` / `sudo passwd useradd emiliano` / `sudo passwd useradd catalina` / `sudo passwd useradd andres` and press Enter. You are required to enter the password twice. You can use the password `Hello1234`

Note When entering the password, nothing appears on the screen, so type your password and press Enter.

```
useradd: invalid user name 'Andres Olazabal'
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd mane
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd emiliano
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd catalina
[ec2-user@ip-10-0-10-122 ~]$ sudo useradd andres
```

27. To validate that users have been created, enter `sudo cat /etc/passwd | cut -d: -f1` and press Enter to look at the contents of the `/etc/passwd` file.



```
ec2-user@ip-10-0-10-122:~
[ec2-user@ip-10-0-10-122 ~]$ sudo cat /etc/passwd | cut -d: -f1
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
operator
games
ftp
nobody
systemd-network
dbus
rpc
libstoragemgmt
sshd
rngd
chrony
rpcuser
nfsnobody
ec2-instance-connect
postfix
tcpdump
ec2-user
mane
emiliano
```




Task 3: Create Groups

In this section you create groups of users and add users to the groups.

- Sales
- HR
- Finance
- Personnel

Once you've created these groups, you add the users to the proper groups based on the information provided in the table in Task 2.

Note You may have to use `sudo` to complete this exercise if you are not root.

Watch out! Managers are personnel, but not all personnel are managers. Some users belong to multiple groups.

30. To validate that you are in the home folder of your current user, enter `pwd` and press Enter.

```
[ec2-user@ip-10-0-10-122 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-122 ~]$
```

31. To create the groups, enter and press Enter.

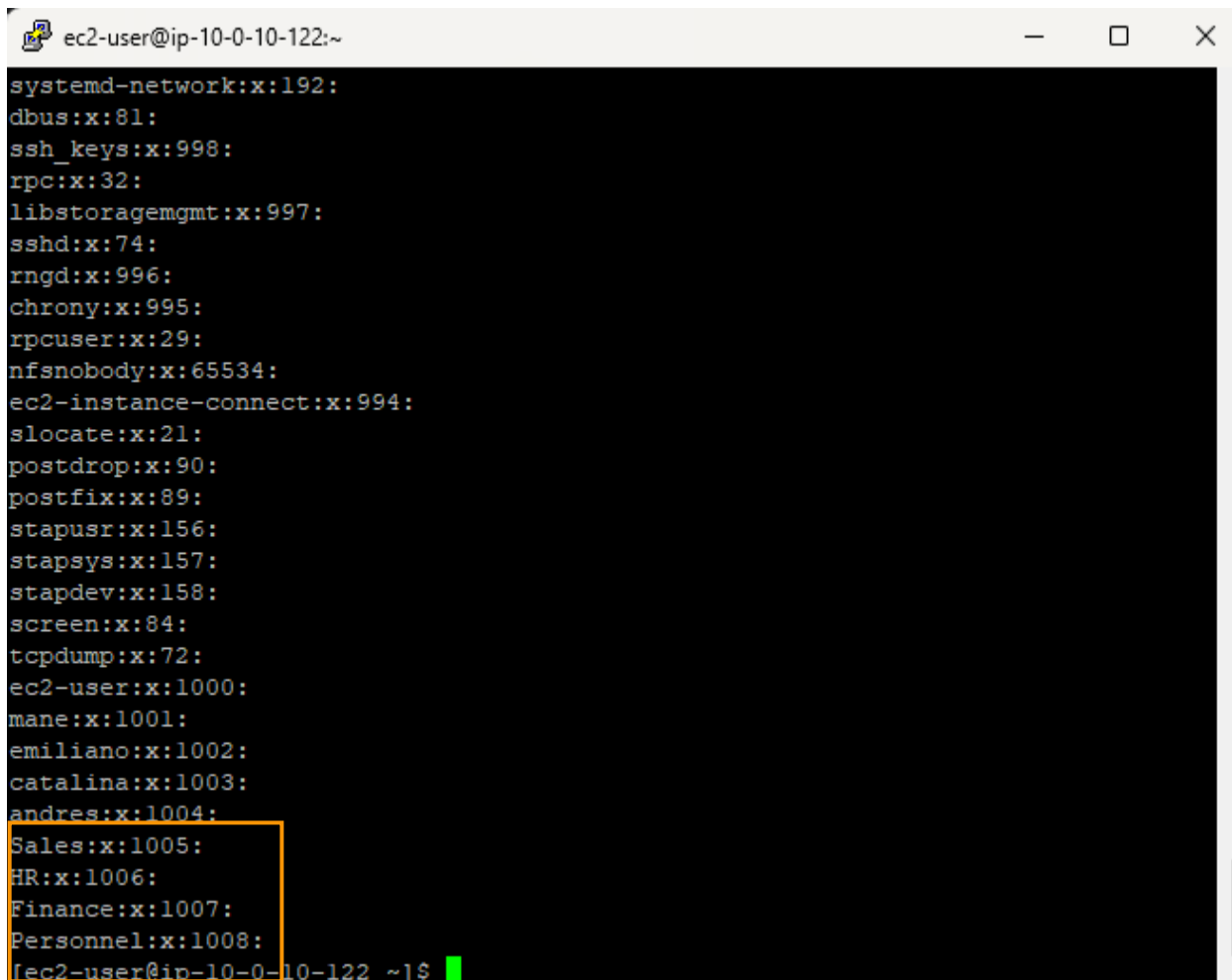
```
sudo groupadd Sales
sudo groupadd HR
sudo groupadd Finance
sudo groupadd Personnel
```

```
[ec2-user@ip-10-0-10-122 ~]$ sudo groupadd Sales
groupadd: group 'Sales' already exists
[ec2-user@ip-10-0-10-122 ~]$ sudo groupadd HR
[ec2-user@ip-10-0-10-122 ~]$ sudo groupadd Finance
[ec2-user@ip-10-0-10-122 ~]$ sudo groupadd Personnel
[ec2-user@ip-10-0-10-122 ~]$
```



32. To verify that the group was added, enter `cat /etc/group` and press Enter.

Note The `/etc/group` file contains all the groups. You should notice that there is already one group for each user that you created earlier because a group is created for each new user. You may have different numbers than the ones displayed. Don't worry about other information behind the first colon. You will learn about the format of the `/etc/group` later.



```
ec2-user@ip-10-0-10-122:~  
systemd-network:x:192:  
dbus:x:81:  
ssh_keys:x:998:  
rpc:x:32:  
libstoragemgmt:x:997:  
sshd:x:74:  
rngd:x:996:  
chrony:x:995:  
rpcuser:x:29:  
nfsnobody:x:65534:  
ec2-instance-connect:x:994:  
slocate:x:21:  
postdrop:x:90:  
postfix:x:89:  
stapusr:x:156:  
stapsys:x:157:  
stapdev:x:158:  
screen:x:84:  
tcpdump:x:72:  
ec2-user:x:1000:  
mane:x:1001:  
emiliano:x:1002:  
catalina:x:1003:  
andres:x:1004:  
Sales:x:1005:  
HR:x:1006:  
Finance:x:1007:  
Personnel:x:1008:  
[ec2-user@ip-10-0-10-122 ~]$
```



33. To add the user **mane** to the **Sales** group, enter `sudo usermod -a -G Sales mane` into the terminal and press Enter. The same procedure with the following users and their respective groups.

```
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G Sales mane
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G Finance emiliano
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G HR andres
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G Personnel catalina
```

34. To verify that the user was added, enter `cat /etc/group` and press Enter.

```
Sales:x:1005:mane
HR:x:1006:andres
Finance:x:1007:emiliano
Personnel:x:1008:catalina
```

38. Add **ec2-user** to all groups.

```
sudo usermod -a -G Sales ec2-user
sudo usermod -a -G Finance ec2-user
sudo usermod -a -G HR ec2-user
sudo usermod -a -G Personnel ec2-user
```

```
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G Sales ec2-user
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G Finance ec2-user
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G HR ec2-user
[ec2-user@ip-10-0-10-122 ~]$ sudo usermod -a -G Personnel ec2-user
```

39. To check the group memberships, enter `sudo cat /etc/group` into the terminal and press Enter.



Task 4: Log in using the new users

Now that you have some users in your machine, you can log in as a new user. You also see what a sudoer is, what this enables, and how commands issued using **sudo** are logged in the `/var/log/secure` file.

Note

You may have to use **sudo** to complete this exercise if you are not root.

40. Enter **su andres**

41. For the password, enter `Hello1234` and press Enter. You are now logged in as **andres**.

The trailing **ec2-user** indicates that you are located in the ec2-user home directory, `/home/ec2-user`.

```
[ec2-user@ip-10-0-10-122 ~]$ su andres
Password:
[andres@ip-10-0-10-122 ec2-user]$
```

42. Enter **pwd** and press Enter to ensure that you are in the `/home/ec2-user` directory.

```
[andres@ip-10-0-10-122 ec2-user]$ pwd
/home/ec2-user
```

43. Enter **touch myFile.txt** and press Enter.

```
[arosalez@ec2-user]$ touch myFile.txt
touch: cannot touch 'myFile.txt': Permission denied
```

You receive this message because the user **andres** does not have permission to write files to the **ec2-user** home folder.

```
[andres@ip-10-0-10-122 ec2-user]$ touch myFile.txt
touch: cannot touch 'myFile.txt': Permission denied
```



44. Now you try as an admin using the `sudo` command. Enter `sudo touch myFile.txt` and press Enter.

```
[andres@ip-10-0-10-117 ec2-user]$ touch myFile.txt
touch: cannot touch 'myFile.txt': Permission denied
[andres@ip-10-0-10-117 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 andres:
andres is not in the sudoers file. This incident will be reported.
[andres@ip-10-0-10-117 ec2-user]$
```

45. Enter the password `Hello1234` and press Enter.

```
[andres@ec2-user]$ touch myFile.txt
andres is not in the sudoers file. This incident will be reported.
```

You receive this message because the user **andres** is not on the list of the sudoers file. Sudoers are users who have special rights to run commands that require root rights. Only a few users should receive this permission.

46. Enter `exit` and press Enter to switch to the previous user, **ec2-user**.

```
[andres@ip-10-0-10-117 ec2-user]$ exit
exit
```

47. Now you visualize the content of the `/var/log/secure` file. Enter `sudo cat /var/log/secure` and press Enter to display the content of the secure file. Scroll to the bottom of the file using the down arrow:

You can see how a `sudo` and not permitted action was logged into the `/var/log/secure` file



```
ec2-user@ip-10-0-10-117:~$ sudo cat /var/log/secure
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: new group: name=ec2-user, GID=1000
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: new user: name=ec2-user, UID=1000,
GID=1000, home=/home/ec2-user, shell=/bin/bash
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: add 'ec2-user' to group 'adm'
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: add 'ec2-user' to group 'wheel'
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: add 'ec2-user' to group 'systemd-j
ournal'
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: add 'ec2-user' to shadow group 'ad
m'
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: add 'ec2-user' to shadow group 'wh
eel'
Oct 26 00:24:40 ip-10-0-10-117 useradd[2197]: add 'ec2-user' to shadow group 'sy
stemd-journal'
Oct 26 00:24:41 ip-10-0-10-117 sshd[2277]: Server listening on 0.0.0.0 port 22.
Oct 26 00:24:41 ip-10-0-10-117 sshd[2277]: Server listening on :: port 22.
Oct 26 00:24:41 ip-10-0-10-117 sshd[2277]: Received signal 15; terminating.
Oct 26 00:24:41 ip-10-0-10-117 sshd[2297]: Server listening on 0.0.0.0 port 22.
Oct 26 00:24:41 ip-10-0-10-117 sshd[2297]: Server listening on :: port 22.
Oct 26 00:26:02 ip-10-0-10-117 sshd[2365]: Accepted publickey for ec2-user from
167.57.251.165 port 56782 ssh2: RSA SHA256:zNv7PwrfxdvzGwxoFbRmmVBAQgJ3p3AMjJeEc
28upSo
Oct 26 00:26:02 ip-10-0-10-117 sshd[2365]: pam_unix(sshd:session): session opene
d for user ec2-user by (uid=0)
Oct 26 00:34:25 ip-10-0-10-117 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ;
USER=root ; COMMAND=/sbin/useradd#040andres
Oct 26 00:34:25 ip-10-0-10-117 sudo: pam_unix(sudo:session): session opened for
user root by ec2-user(uid=0)
```

Lab Complete



Congratulations! You have completed the lab.

48. Choose **End Lab** at the top of this page, and then select **Yes** to confirm that you want to end the lab.

A panel indicates that *DELETE has been initiated... You may close this message box now.*

49. A message *Ended AWS Lab Successfully* is briefly displayed, indicating that the lab has ended.



Commands Used:

On this lab we used several commands to perform different tasks. Here is a summary of the commands used:

Command	Description
<code>pwd</code>	Displays the current directory.
<code>sudo useradd username</code>	Creates new users.
<code>sudo passwd username</code>	Sets passwords for the created users.
<code>sudo cat /etc/passwd</code>	Lists user accounts to confirm they were created.
<code>sudo groupadd GroupName</code>	Creates groups for users.
<code>cat /etc/group</code>	Lists all groups in the system.
<code>sudo usermod -a -G GroupName username</code>	Adds users to specific groups.
<code>sudo cat /etc/group</code>	Displays group memberships for verification.
<code>su username</code>	Switches to a new user.
<code><Password></code>	Logs in using the user's password.
<code>touch myFile.txt</code>	Tries to create a file as the new user (permission denied).
<code>sudo touch myFile.txt</code>	Creates a file with sudo rights.
<code>exit</code>	Switches back to the previous user.
<code>sudo cat /var/log/secure</code>	Displays the log of sudo actions.