Managing Users and Groups

> **Note**
>
> All labs rely on previous courseware and lab information.

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

Duration

This lab requires approximately **45 minutes** to complete.

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that you need to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that this lab describes.

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 along side 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. The following instructions vary slightly depending on whether you are using Windows or Mac/Linux.

Windows Users: Using SSH to Connect

These instructions are specifically for Windows users. If you are using macOS or Linux, skip to the next section.

5. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
6. Select the **Download PPK** button and save the **labsuser.ppk** file.
   Typically your browser will save it to the Downloads directory.
7. Make a note of the **PublicIP** address.
8. Then exit the Details panel by selecting the **X**.
9. Download **PuTTY** to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer, download it here.
10. Open **putty.exe**
11. Configure PuTTY timeout to keep the PuTTY session open for a longer period of time.:
    - Select **Connection**
    - Set **Seconds between keepalives** to `30`
12. 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**
    - Select **Auth** *(don't expand it)*
    - Select **Browse**
    - Browse to and select the lab#.ppk file that you downloaded
    - Select **Open** to select it
    - Select **Open** again.
13. Select **Yes**, to trust and connect to the host.
14. When prompted **login as**, enter: `ec2-user`
    This will connect you to the EC2 instance.

15. Windows Users: Select here to skip ahead to the next task.

macOS and Linux Users

These instructions are specifically for Mac/Linux users. If you are a Windows user, skip ahead to the next task.

16. Select the Details drop-down menu above these instructions you are currently reading, and then select Show. A Credentials window will be presented.
17. Select the **Download PEM** button and save the **labsuser.pem** file.
18. Make a note of the **PublicIP** address.
19. Then exit the Details panel by selecting the **X**.
20. Open a terminal window, and change directory `cd` to the directory where the *labsuser.pem* file was downloaded. For example, if the *labuser.pem* file was saved to your Downloads directory, run this command:

```
cd ~/Downloads
```

21. Change the permissions on the key to be read-only, by running this command:

```
chmod 400 labsuser.pem
```

22. Run the below command *(replace **<public-ip>** with the **PublicIP** address you copied 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.:

```
ssh -i labsuser.pem ec2-user@<public-ip>
```

23. Type `yes` when prompted to allow the first connection to this remote SSH server.
Because you are using a key pair for authentication, you will not be prompted for a password.

Task 2: Create Users

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

First Name	Last Name	User ID	Job Role	Starting Password
Alejandro	Rosalez	arosalez	Sales Manager	P@ssword1234!
Efua	Owusu	eowusu	Shipping	P@ssword1234!
Jane	Doe	jdoe	Shipping	P@ssword1234!
Li	Juan	ljuan	HR Manager	P@ssword1234!
Mary	Major	mmajor	Finance Manager	P@ssword1234!
Mateo	Jackson	mjackson	CEO	P@ssword1234!
Nikki	Wolf	nwolf	Sales Representative	P@ssword1234!
Paulo	Santos	psantos	Shipping	P@ssword1234!
Sofia	Martinez	smartinez	HR Specialist	P@ssword1234!
Saanvi	Sarkar	ssarkar	Finance Specialist	P@ssword1234!

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]$
```

25. To add the first user from the list above, **Alejandro Rosalez**, enter `sudo useradd arosalez` and press Enter.
    This step creates the user **arosalez**.

26. Enter `sudo passwd arosalez` and press Enter.
    You are required to enter the password twice. You can use the password `P@ssword1234!`

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

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]$ sudo cat/etc/passwd | cut -d: -f1
........
ec2-user
arosalez
```

> **Note**

> This command helps visualize the created users and is not necessary for you to remember for now. **cat** is one of the most popular command. One of its purposes is to display files. You can also enter `cat /etc/passwd` to display the whole content of the file, but this option displays more information and is less readable. Don't bother with the second part of the command for now. You will learn more about the **cat**, **cut**, and **|** commands later in this course.

28. Use the `sudo useradd <User ID>` and `sudo passwd <User ID>` commands to add the remaining users from the table. Replace *<User ID>* with each **User ID** in the table at the beginning of this task.
29. To validate that all users have been created, enter `sudo cat /etc/passwd | cut -d: -f1` and press Enter.

```
[ec2-user]$ sudo cat /etc/passwd | cut -d: -f1
........
ec2-user
arosalez
eowusu
jdoe
ljuan
mjackson
mmajor
nwolf
psantos
smartinez
ssarkar
```

Task 3: Create Groups

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

- **Sales**
- **HR**
- **Finance**
- **Personnel**
- **CEO**
- **Shipping**
- **Managers**

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.
31. To create the **Sales** group, enter `sudo groupadd Sales` and press Enter.
32. To verify that the group was added, enter `cat /etc/group` and press Enter.

```
...
ec2-user:x:1000:
......
Sales:x:1014
....
```

> **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.

33. Use the `sudo groupadd <Group>` command to add the remaining groups. Replace <*Group*> with **HR**, **Finance**, **Shipping**, and **Managers** and **CEO** to create these groups.
34. To verify that all the groups were added, enter `cat /etc/group` and press Enter.

```
Sales:x:1014
HR:x:1015
Finance:x:1016
Shipping:x:1017
Managers:x:1018
CEO:x:1019
```

35. To add the user **arosalez** to the **Sales** group, enter `sudo usermod -a -G Sales arosalez` into the terminal and press Enter.
36. To verify that the user was added, enter `cat /etc/group` and press Enter.

```
....
Sales:x:1014:arosalez
....
```

37. Use the `sudo usermod -a -G <Group Name> <User ID>` command to add the remaining users to the appropriate groups. Using the information in the following table, replace <*Group Name*> with the **Group Name**, and replace <*User ID*> with each user ID in the **User IDs** columns.

Group Name	User IDs	Group Name	User IDs	Group Name	User IDs
Sales	arosaleznwolf	HR	ljuansmartinez	Finance	mmajors
Shipping	eowusujdoepsantos	Managers	arosalezljuanmmajor	CEO	mjackso

38. Add ec2-user to all groups.
39. To check the group memberships, enter `sudo cat /etc/group` into the terminal and press Enter.

```
Sales:x:1014:arosalez,nwolf,ec2-user
HR:x:1015:ljuan,smartinez,ec2-user
Finance:x:1016:mmajor,ssarkar,ec2-user
Shipping:x:1017:eowusu,jdoe,psantos,ec2-user
Managers:x:1018:arosalez,ljuan,mmajor,ec2-user
CEO:x:1019:mjackson,ec2-user
```

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 arosalez**
41. For the password, enter `P@ssword1234!` and press Enter.
    You are now logged in as **arosalez**.

    ```
    [arosalez@ec2-user]$
    ```

    The trailing **ec2-user** indicates that you are located in the ec2-user home directory, **/home/ec2-user**.
42. Enter `pwd` and press Enter to ensure that you are in the **/home/ec2-user** directory.
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 **arosalez** does not have permission to write files to the **ec2-user** home folder.
44. Now you try as an admin using the **sudo** command. Enter `sudo touch myFile.txt` and press Enter.
45. Enter the password **P@ssword1234!** and press Enter.

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

    You receive this message because the user **arosalez** 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**.
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:

```
Aug  9 14:45:55 ip-10-0-10-217 sudo: arosalez : user NOT in sudoers ; TTY=pts/1
; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/touch myFile.txt
```

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

Lab Complete

Congratulations! You have completed the lab.

48. Select End Lab at the top of this page and then select **Yes** to confirm that you want to end the lab.
    A panel will appear, indicating that "DELETE has been initiated... You may close this message box now."
49. Select the **X** in the top right corner to close the panel.

About the AWS component:

Amazon EC2 provides a wide selection of *instance types* optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more *instance sizes* so that you can scale your resources to the requirements of your target workload.

This lab uses a **t3.micro** instance, which should be selected by default. This instance type has 1 virtual CPU and 1 GiB of memory.

Additional Resources

- Amazon EC2 Instance Types
- Amazon Machine Images (AMI)
- Status Checks for Your Instances
- Amazon EC2 Service Limits
- Terminate Your Instance

For more information about AWS Training and Certification, see https://aws.amazon.com/training/.

Your feedback is welcome and appreciated.
If you would like to share any suggestions or corrections, please provide the details in our AWS Training and Certification Contact Form.