Ivan Castillo

Gestión de procesos

Objetivos

En este laboratorio usted:

- Cree un nuevo archivo de registro para listados de procesos
- Utilice el comando superior
- Establezca una tarea repetitiva que ejecute sus comandos de auditoría anteriores una vez al día.

Los siguientes componentes se crean para usted como parte del entorno de laboratorio :

Amazon EC2: host de comandos (en la subred pública): inicie sesión en esta instancia para utilizar los comandos enumerados en esta práctica de laboratorio.

Tarea 1: utilizar SSH para conectarse a una instancia EC2 de Amazon Linux

En esta tarea, se conectará a una instancia EC2 de Amazon Linux. Utilizará una utilidad SSH para realizar todas estas operaciones. Las siguientes instrucciones varían ligeramente dependiendo de si está utilizando Windows o Mac/Linux.

USUARIOS DE WINDOWS: USO DE SSH PARA CONECTARSE

Estas instrucciones son específicamente para usuarios de Windows. Si está utilizando macOS o Linux, pase a la siguiente sección.

3. En el panel **Información del laboratorio** , seleccione el enlace **PPK** y guarde el archivo. El nombre del archivo será similar a *Ec2KeyPair-PPK.ppk* . *Normalmente su navegador lo guardará en el directorio de Descargas.*

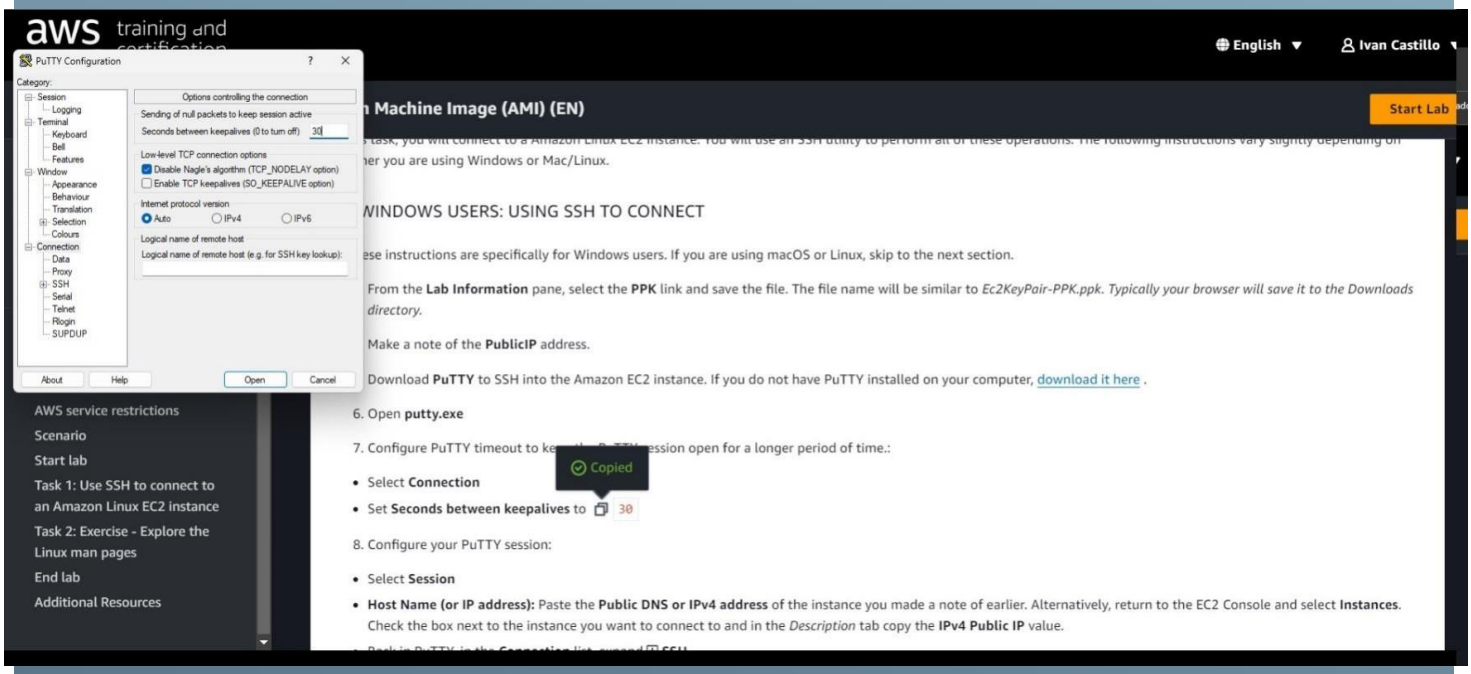
4. Tome nota de la dirección **PublicIP** .

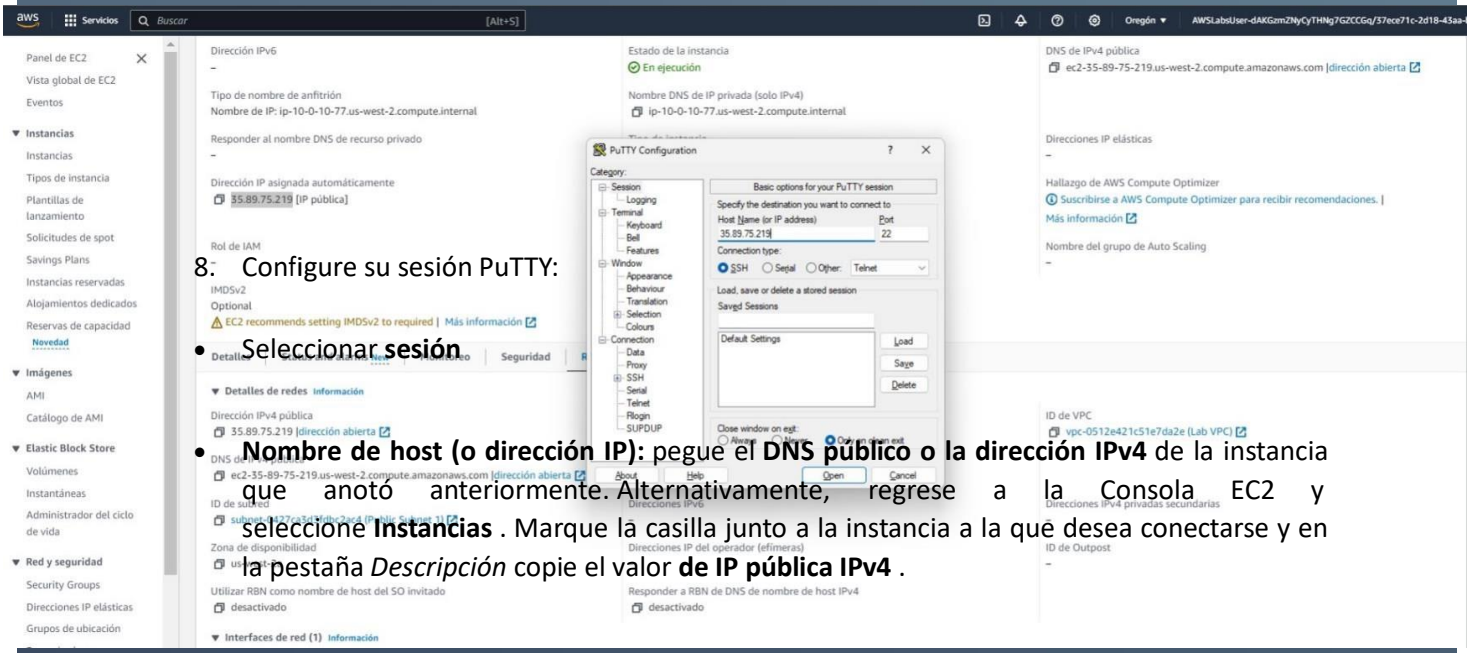
5. Descargue **PuTTY** a SSH en la instancia de Amazon EC2.

6. Abrir **PuTTY .exe**

7. Configure el tiempo de espera de PuTTY para mantener abierta la sesión de PuTTY durante un período de tiempo más largo:

- Seleccionar **conexión**





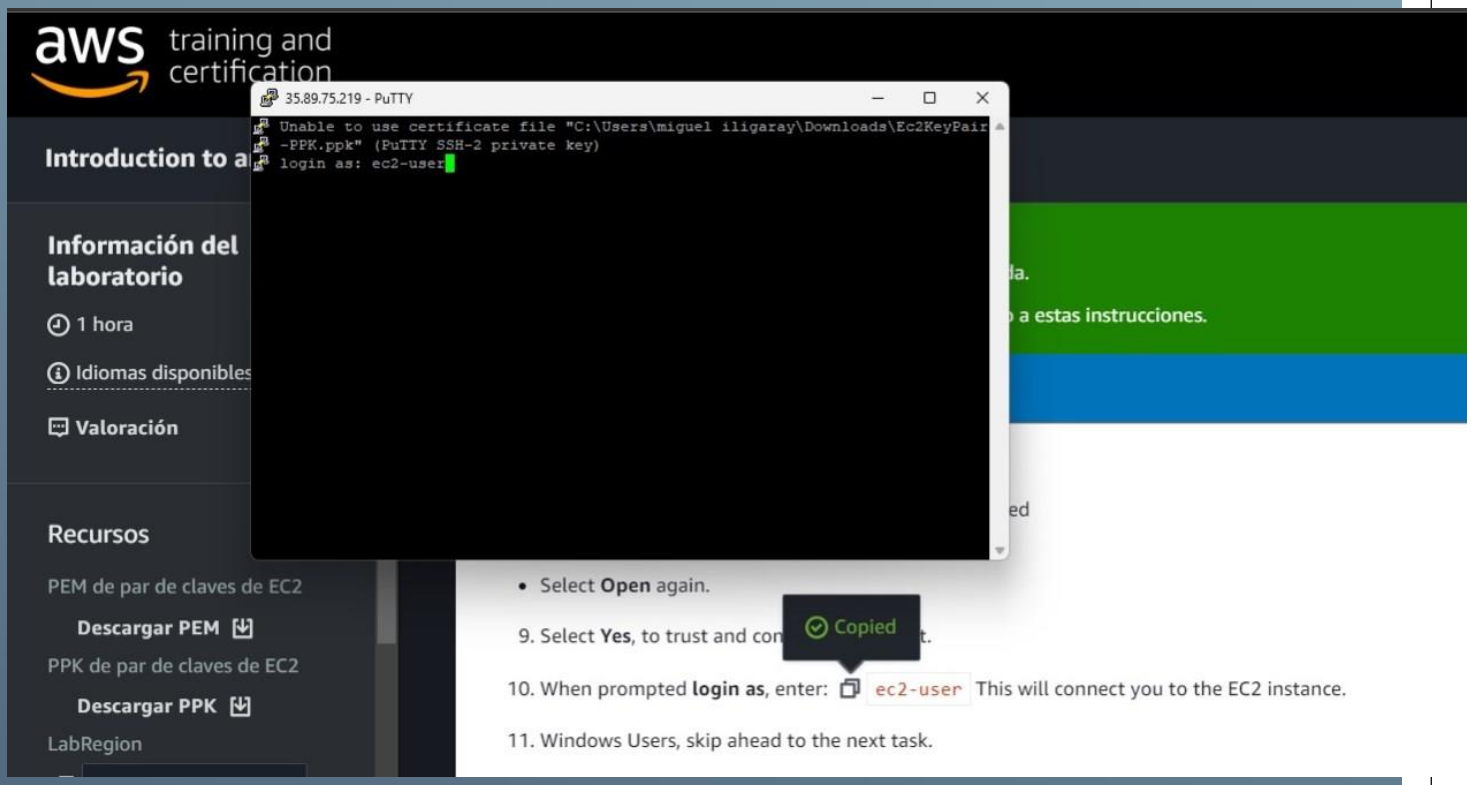
8. Configure su sesión PuTTY:

- Seleccionar **sesión**
- **Nombre de host (o dirección IP):** pegue el **DNS público o la dirección IPv4** de la instancia que anotó anteriormente. Alternativamente, regrese a la Consola EC2 y seleccione **Instancias** . Marque la casilla junto a la instancia a la que desea conectarse y en la pestaña *Descripción* copie el valor **de IP pública IPv4** .

10. Cuando se le solicite **iniciar sesión como** , ingrese:

ec2-user

Esto lo conectará a la instancia EC2.



Tarea 2: Ejercicio: crear una lista de procesos

En este ejercicio, creará un archivo de registro a partir del comando ps. Este archivo de registro debe agregarse a la sección SharedFolders:

Cree un archivo de registro llamado procesos.csv desde ps -aux y omita cualquier proceso que contenga usuario root o contenga "["o"]" en la sección COMANDO.

Nota : hay un espacio después del comando seguido de un punto para representar la ubicación actual.

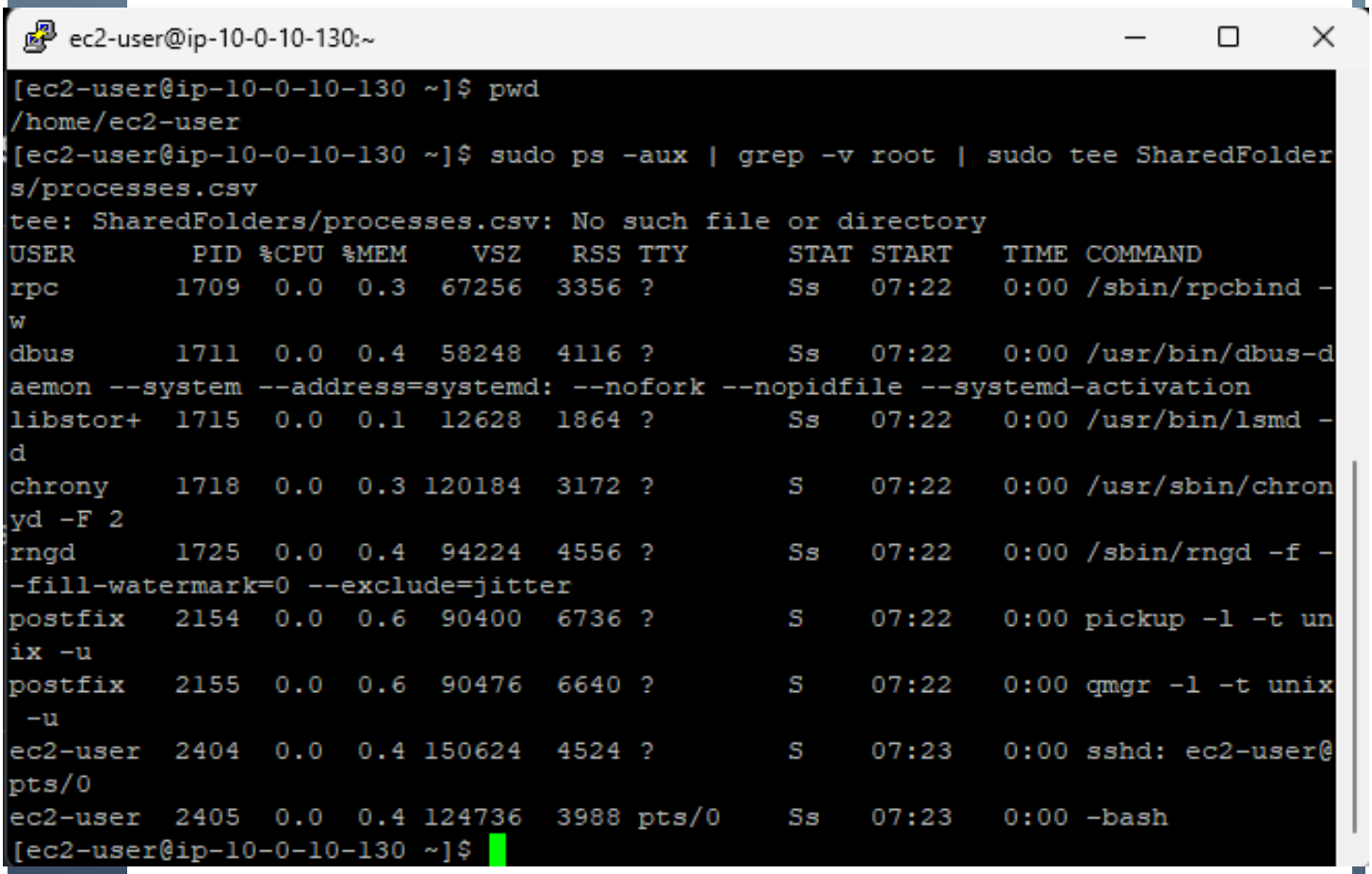
18. Para validar que estás en el `/home/ec2-user/companyA` carpeta, ingrese `pwd`

y presione Entrar.

Si no estás en esta carpeta, ingresa `cd companyA` y presione Entrar.

19. Vea todos los procesos que se ejecutan en la máquina y filtre la palabra raíz escribiendo `sudo ps -aux | grep -v root | sudo tee SharedFolders/processes.csv` y presionando ENTER.

20. Valida tu trabajo escribiendo `cat SharedFolders/processes.csv` y presionando ENTER.



Tarea 3: Ejercicio: enumerar los procesos usando el comando superior

En este ejercicio, utilizará el comando superior:

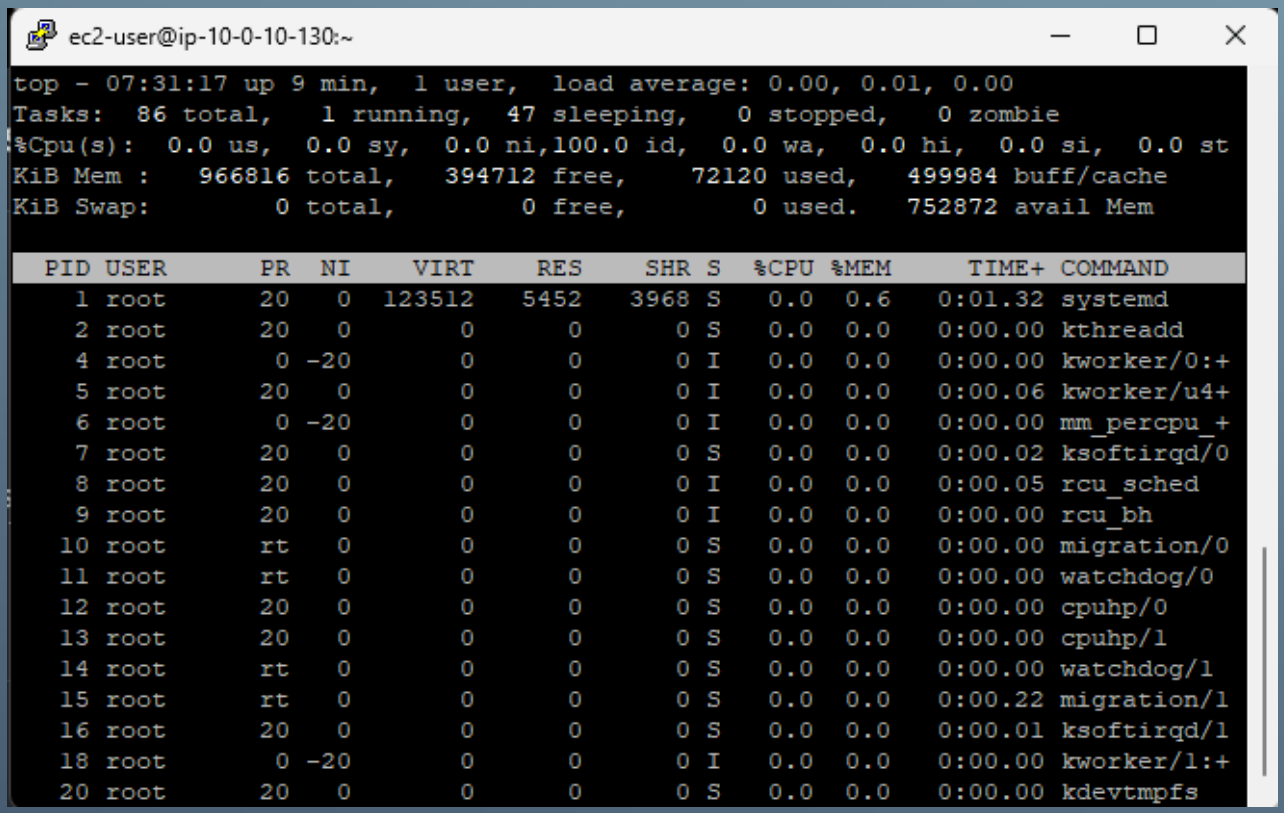
- Ejecute el comando **superior** para mostrar los procesos y subprocesos que están activos en el sistema.
- Observe los resultados del comando superior.

21. En la terminal principal ejecute el comando top y presione ENTER:

```
top
```

El comando superior se utiliza para mostrar el rendimiento del sistema y enumera los procesos y subprocesos activos en el sistema.

Mientras observamos el resultado de top, la segunda línea debajo del comando top, podemos ver las Tareas. Las tareas en la parte superior tienen un estado de ejecución, suspensión, detención o zombie.



23. Para salir de la parte superior, presione **q** y presione ENTER.

24. También puede ejecutar top con las siguientes opciones para encontrar información de uso y versión: top -hv

Tarea 4: Ejercicio: crear un trabajo cron

En este ejercicio, creará un trabajo cron que creará un archivo de auditoría con ##### para cubrir todos los archivos csv:

Nota : Es posible que tengas que usar sudo para completar este ejercicio si no eres root.

Recuerde que **cron** es un comando que ejecuta una tarea de forma regular a una hora específica. Este comando mantiene la lista de tareas para ejecutar en un archivo crontab, que crea en esta tarea. Crea un trabajo que crea el archivo de auditoría con ##### para cubrir todos los archivos .csv. Cuando ingresa el comando **crontab -e** , se lo lleva a un editor donde luego ingresa una lista de pasos de lo que ejecutará el demonio cron. El archivo crontab incluye seis campos: minutos, hora, día del mes (DOM), mes (MON), día de la semana (DOW) y comando (CMD). Estos campos también se pueden indicar con asteriscos. Una vez que se ejecute este comando, podrá verificar su trabajo.

25. Para validar que estás en el `/home/ec2-user/ companyA` carpeta, ingrese `pwd` y presione Entrar.

26. Para crear un trabajo cron que cree el archivo de auditoría con ##### para cubrir todos los archivos .csv, ingrese `sudo crontab-e` y presione Enter para ingresar al editor de texto predeterminado.

27. Prensa `i` para ingresar al modo de inserción y presione Entrar.

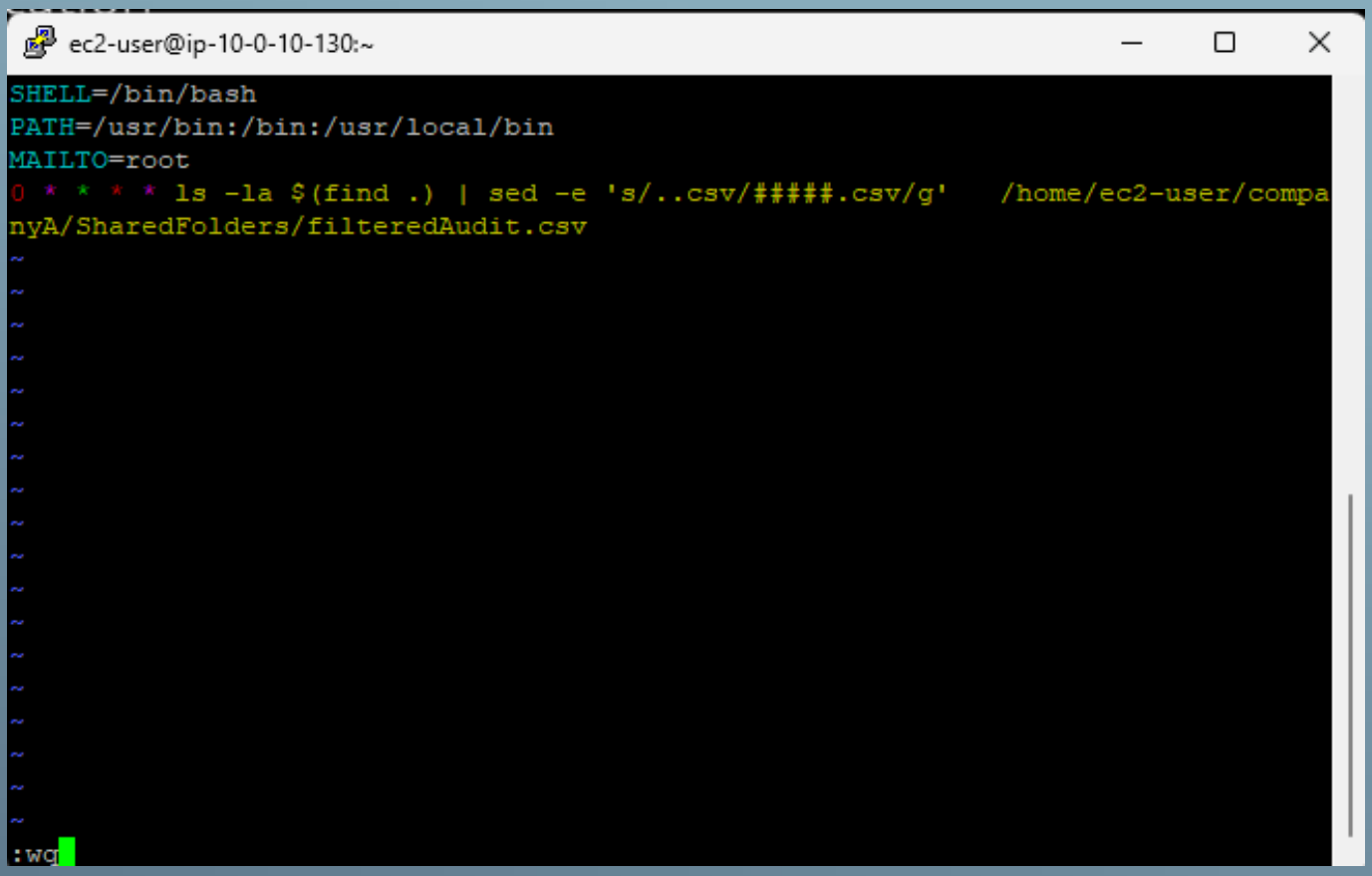
28. Para la primera línea, ingrese `SHELL=/bin/bash` y presione la barra espaciadora.

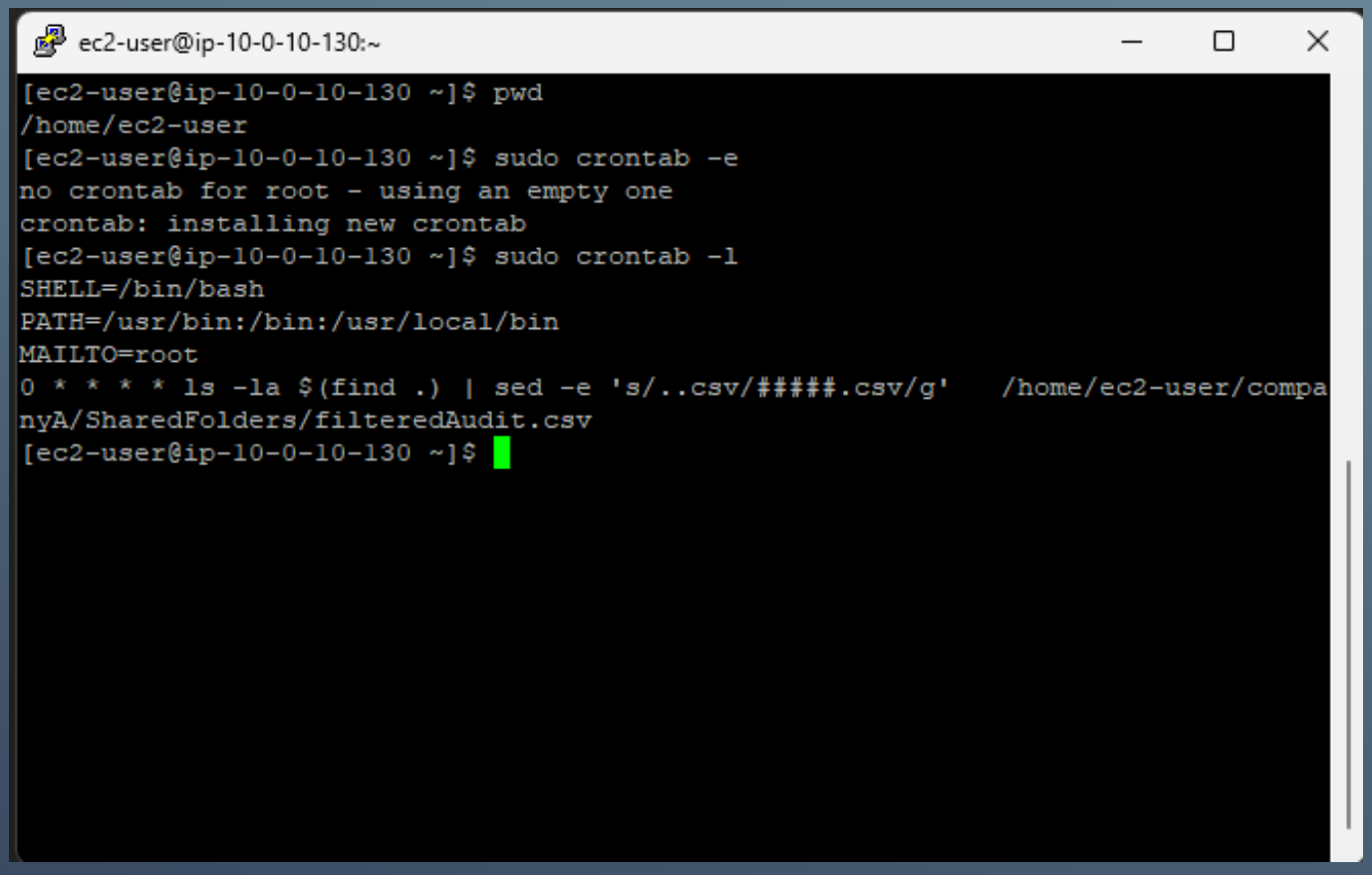
29. Para la segunda línea, ingrese `RUTA=/usr/bin:/bin:/usr/local/bin`

    y presione Entrar.

30. Para la tercera línea, ingrese `MAILTO=root` y presione Entrar.

31. Para la última línea, ingrese `0 * * * * ls -la $(find .) | sed -e 's/..csv/#####.csv/g'  /home/ec2 -user/companyA/SharedFolders/filteredAudit.csv`


ec2-user@ip-10-0-10-130:~
SHELL=/bin/bash
PATH=/usr/bin:/bin:/usr/local/bin
MAILTO=root
0 * * * * ls -la $(find .) | sed -e 's/../csv/#####.csv/g' /home/ec2-user/compa
nyA/SharedFolders/filteredAudit.csv
:wq


ec2-user@ip-10-0-10-130:~
[ec2-user@ip-10-0-10-130 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-130 ~]$ sudo crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
[ec2-user@ip-10-0-10-130 ~]$ sudo crontab -l
SHELL=/bin/bash
PATH=/usr/bin:/bin:/usr/local/bin
MAILTO=root
0 * * * * ls -la $(find .) | sed -e 's/../csv/#####.csv/g' /home/ec2-user/compa
nyA/SharedFolders/filteredAudit.csv
[ec2-user@ip-10-0-10-130 ~]$