Laboratorio

Managing Processes

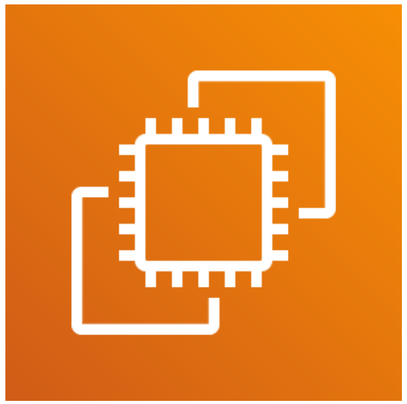
Hecho con amor por:
Agustín Rodriguez, Cristofer Gutiérrez,
Fernanda Urman, Gonzalo Rondeau y Nacho Suárez

Objetivos

- Crear un archivo de registro nuevo para las listas de procesos
- Utilizar el comando top
- Establecer una tarea repetitiva que ejecute los comandos de auditoría anteriores una vez al día

1: Conexión con instancia EC2

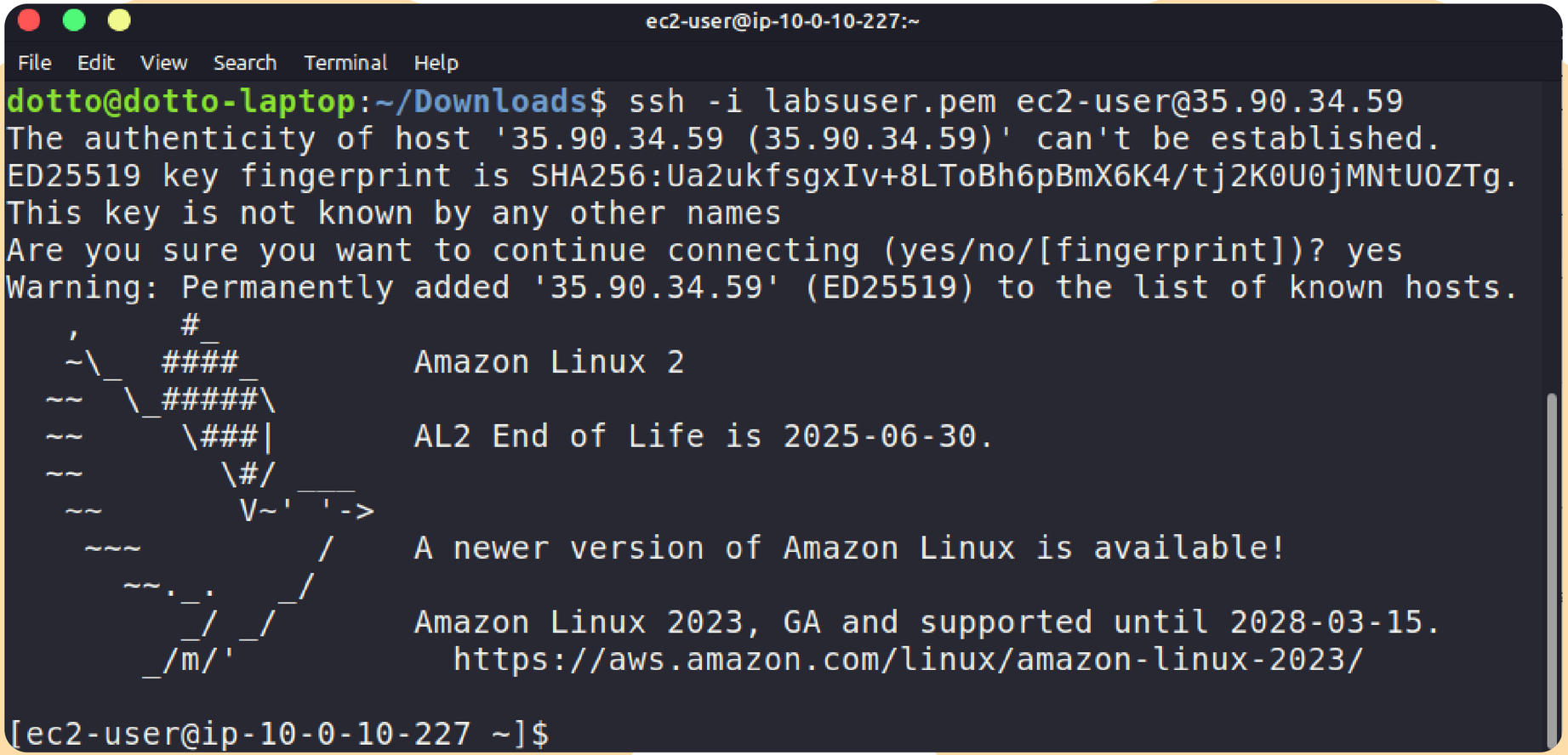
- Esperaremos a que la instancia esté cargada y nos conectaremos a ella mediante SSH.



Amazon EC2

- En Windows: usando PuTTY
- En Linux: con el comando ssh

Conexión con la instancia.



2: Crear lista de procesos

- En este ejercicio, haremos un archivo de registro a partir de la salida del comando ps.

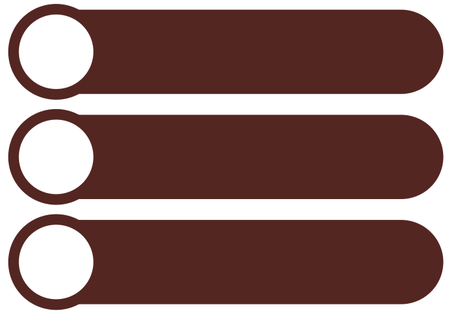
- El archivo de log se llamará processes.csv

Metiendo los procesos al archivo.

```
[ec2-user@ip-10-0-10-18 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-18 ~]$ cd comapnyA
-bash: cd: comapnyA: No such file or directory
[ec2-user@ip-10-0-10-18 ~]$ cd companyA
[ec2-user@ip-10-0-10-18 companyA]$ sudo ps -aux | grep -v  root | sudo tee Share
dFolders/processes.csv
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
libstor+   1706  0.0  0.2  12628  1936 ?        Ss   22:37   0:00 /usr/bin/lsmd -
d
rpc        1711  0.0  0.3  67256  3292 ?        Ss   22:37   0:00 /sbin/rpcbind -
w
dbus       1721  0.0  0.4  58248  4132 ?        Ss   22:37   0:00 /usr/bin/dbus-d
aemon --system --address=systemd: --nofork --nopidfile --systemd-activation
chrony     1735  0.0  0.3 120184  3168 ?        S    22:37   0:00 /usr/sbin/chron
yd -F 2
rngd       1748  0.0  0.4  96344  4716 ?        Ss   22:37   0:00 /sbin/rngd -f -
-fill-watermark=0 --exclude=jitter
postfix    2160  0.0  0.6  90396  6716 ?        S    22:37   0:00 pickup -l -t un
ix -u
postfix    2161  0.0  0.7  90468  6824 ?        S    22:37   0:00 qmgr -l -t unix
 -u
ec2-user   2899  0.0  0.4 148520  4728 ?        S    22:38   0:00 sshd: ec2-user@
pts/0
ec2-user   2900  0.0  0.4 124736  3964 pts/0    Ss   22:38   0:00 -bash
[ec2-user@ip-10-0-10-18 companyA]$
```

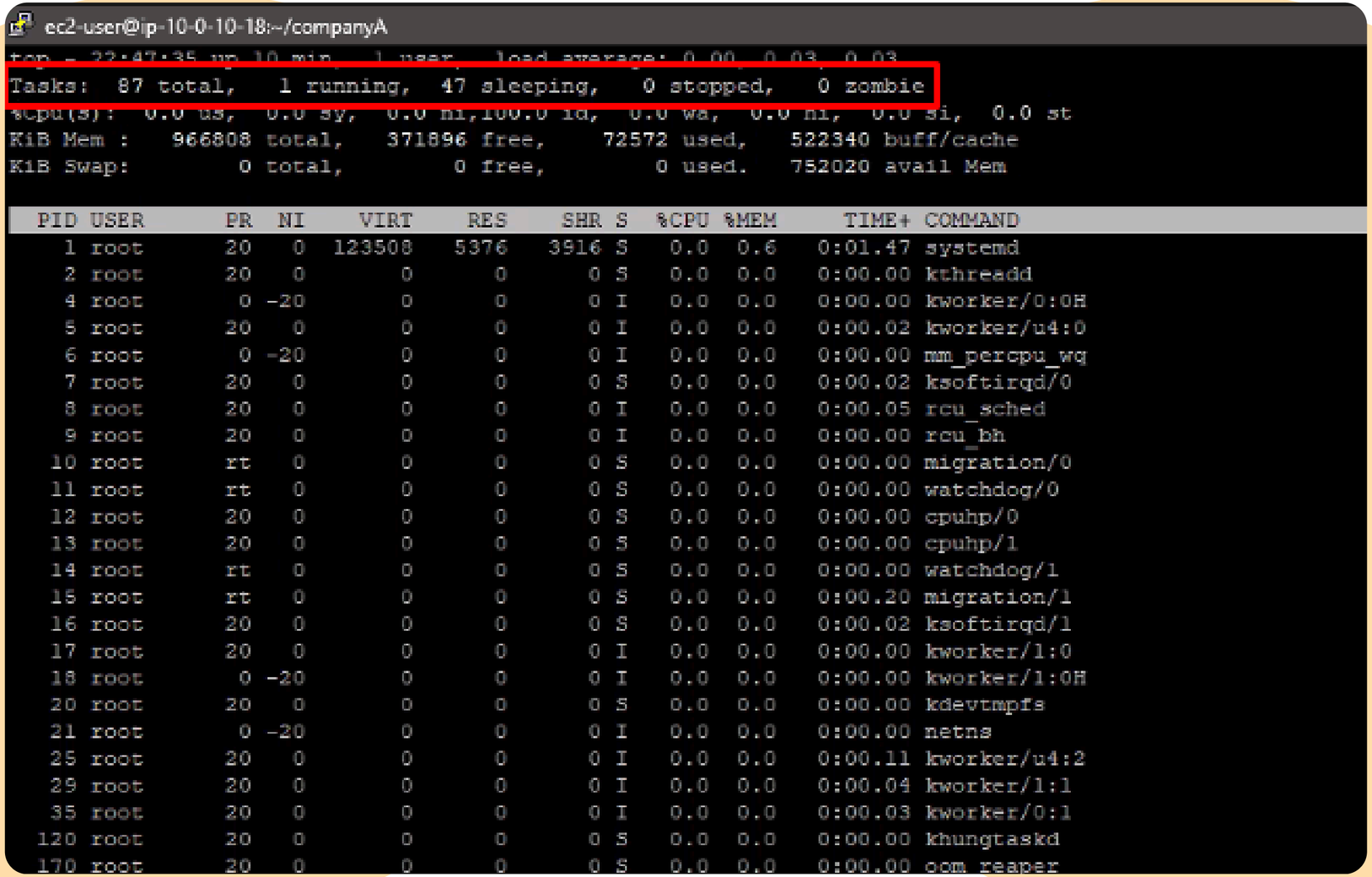
3: Listar los procesos

- Usaremos el comando de top para listar los procesos e hilos activos del sistema.



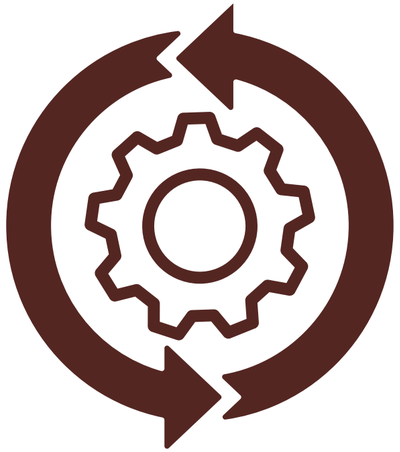
- Nos daremos cuenta de la gran cantidad de procesos que existen, por más de que estos no sean visibles.

Lista de procesos en top.



4: Crear un proceso Cron

- Usaremos el comando cron, este comando sirve para programar tareas y que se ejecuten en momentos específicos.



- Crearemos una tarea que ejecute los comandos del día anterior del archivo de auditoria.

Creación del cron

```
ec2-user@ip-10-0-10-18:~/companyA
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/comapnyA/SharedFolders/filteredAudit.csv
~
~
```

```
ec2-user@ip-10-0-10-18:~/companyA
[ec2-user@ip-10-0-10-18 companyA]$ sudo crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
[ec2-user@ip-10-0-10-18 companyA]$ sudo crontab -l
SHELL=/bin/bash
PATH=/usr/bin:/bin:/usr/local/bin
MAILTO=root
0 * * * * ls -la $(find .) | sed -e 's/..csv/#####.csv/g' > /home/ec2-user/comap
nyA/SharedFolders/filteredAudit.csv
[ec2-user@ip-10-0-10-18 companyA]$
```

Conclusiones

- Cumplimos con los objetivos del laboratorio.
- Aprendimos a usar y manejar información de comandos útiles, tales como: top, ps, etc.

¡Muchas Gracias!