

Laboratorio

Managing Processes



Amazon
Linux

Hecho con amor por:

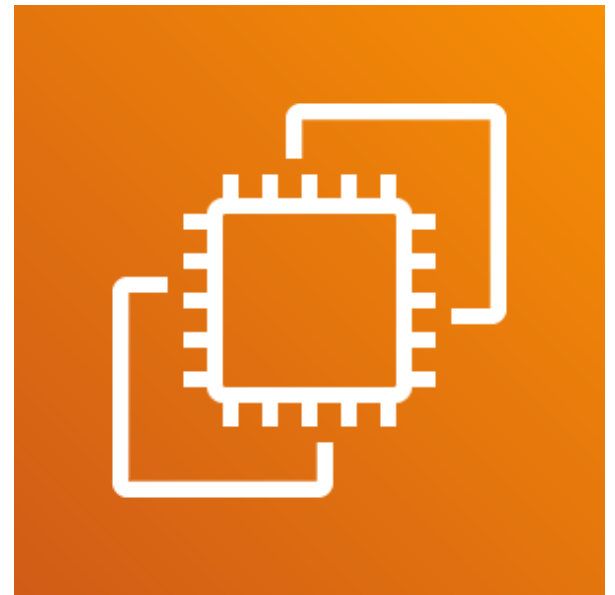
**Agustín Rodríguez, Cristófer Gutiérrez,
Fernanda Urman, Gonzalo Rondeau y Nacho Suárez**

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



Amazon EC2

Conexión con la instancia.

```
ec2-user@ip-10-0-10-227:~  
File Edit View Search Terminal Help  
dotto@dotto-laptop:~/Downloads$ ssh -i labsuser.pem ec2-user@35.90.34.59  
The authenticity of host '35.90.34.59 (35.90.34.59)' can't be established.  
ED25519 key fingerprint is SHA256:Ua2ukfsgxIv+8LToBh6pBmX6K4/tj2K0U0jMNtU0ZTg.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '35.90.34.59' (ED25519) to the list of known hosts.  
  
#  
~\#####_ Amazon Linux 2  
~~\#####\  
~~\###| AL2 End of Life is 2025-06-30.  
~~\#/V~'->  
~~~~/  
~~././ /  
_/_/_/_ /  
_/m/' /  
  
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-10-0-10-227 ~]$
```

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`

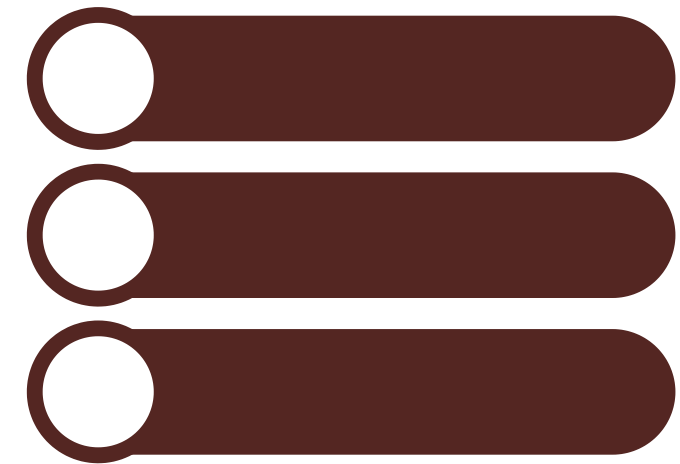


Metiendo los procesos al archivo.

```
[ec2-user@ip-10-0-10-18 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-10-18 ~]$ cd companyA
-bash: cd: companyA: 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.



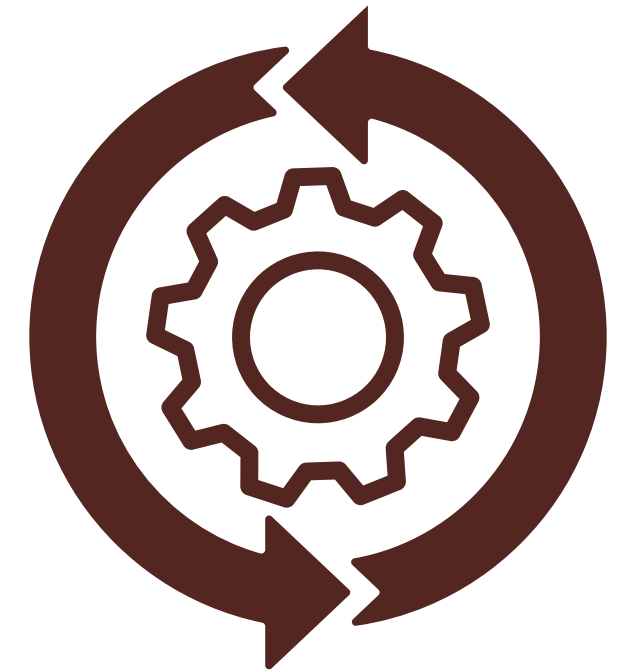
Lista de procesos en top.

```
ec2-user@ip-10-0-10-18:~/companyA
top - 22:47:35 up 10 min, 1 user, load average: 0.00, 0.03, 0.03
Tasks: 87 total, 1 running, 47 sleeping, 0 stopped, 0 zombie
%cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  966808 total,  371896 free,   72572 used,  522340 buff/cache
KiB Swap:         0 total,         0 free,         0 used.  752020 avail Mem
```

| PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|-----|------|----|-----|--------|------|------|---|------|------|---------|--------------|
| 1 | root | 20 | 0 | 123508 | 5376 | 3916 | S | 0.0 | 0.6 | 0:01.47 | systemd |
| 2 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | kthreadd |
| 4 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | kworker/0:0H |
| 5 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.02 | kworker/u4:0 |
| 6 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | mm_percpu_wq |
| 7 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.02 | ksoftirqd/0 |
| 8 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.05 | rcu_sched |
| 9 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | rcu_bh |
| 10 | root | rt | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | migration/0 |
| 11 | root | rt | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | watchdog/0 |
| 12 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | cpuhp/0 |
| 13 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | cpuhp/1 |
| 14 | root | rt | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | watchdog/1 |
| 15 | root | rt | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.20 | migration/1 |
| 16 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.02 | ksoftirqd/1 |
| 17 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | kworker/1:0 |
| 18 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | kworker/1:0H |
| 20 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | kdevtmpfs |
| 21 | root | 0 | -20 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.00 | netns |
| 25 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.11 | kworker/u4:2 |
| 29 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.04 | kworker/1:1 |
| 35 | root | 20 | 0 | 0 | 0 | 0 | I | 0.0 | 0.0 | 0:00.03 | kworker/0:1 |
| 120 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | khungtaskd |
| 170 | root | 20 | 0 | 0 | 0 | 0 | S | 0.0 | 0.0 | 0:00.00 | ocm_reaper |

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 $(find .) | sed -e 's/..csv/####.csv/g' > /home/ec2-user/comapnyA/SharedFolders/filteredAudit.csv
[ec2-user@ip-10-0-10-18 companyA]$
```

Conclusiones

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

¡Muchas Gracias!