

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**

The screenshot shows the AWS training and certification interface. On the left, there's a sidebar with 'AWS service restrictions', 'Scenario', 'Start lab', 'Task 1: Use SSH to connect to an Amazon Linux EC2 Instance', 'Task 2: Exercise - Explore the Linux man pages', 'End lab', and 'Additional Resources'. The main content area is titled 'Machine Image (AMI) (EN)' and contains instructions for connecting to an Amazon EC2 instance using PuTTY. A 'Start Lab' button is visible in the top right. The instructions include steps for downloading PuTTY, configuring it, and connecting to the instance. A 'Copied' tooltip is visible over the '30' value in the 'Seconds between keepalives' field.

PUTTY Configuration

Category: Session

Options controlling the connection

Sending of null packets to keep session active

Seconds between keepalives (0 to turn off) **30**

Low-level TCP connection options

☒ Disable Nagle's algorithm (TCP_NODELAY option)

☐ Enable TCP keepalives (SO_KEEPALIVE option)

Internet protocol version

☒ Auto ☐ IPv4 ☐ IPv6

Logical name of remote host

Logical name of remote host (e.g. for SSH key lookup):

From the **Lab Information** pane, select the **PPK** link and save the file. The file name will be similar to *Ec2KeyPair-PPK.ppk*. Typically your browser will save it to the Downloads directory.

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

Download **PuTTY** to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer, [download it here](#).

6. Open **putty.exe**

7. Configure PuTTY timeout to keep the 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.

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** .

The screenshot shows the AWS Management Console. The left sidebar contains navigation links for 'Panel de EC2', 'Vista global de EC2', 'Eventos', 'Instancias', 'Tipos de instancia', 'Plantillas de lanzamiento', 'Solicitudes de spot', 'Savings Plans', 'Instancias reservadas', 'Alojamientos dedicados', 'Reservas de capacidad', 'Imágenes', 'AMI', 'Catálogo de AMI', 'Elastic Block Store', 'Volumenes', 'Instancias', 'Administrador del ciclo de vida', 'Red y seguridad', 'Security Groups', 'Direcciones IP elásticas', and 'Grupos de ubicación'. The main content area shows the 'Instancias' page with a table of instances. A 'PUTTY Configuration' window is overlaid on the console, showing the 'Session' category. The 'Host Name (or IP address)' field is set to 'ec2-35-89-75-219.us-west-2.compute.amazonaws.com'. The 'Port' is set to '22'. The 'Connection type' is set to 'SSH'. The 'Seconds between keepalives' is set to '30'. The 'Host Name (or IP address)' field is highlighted with a red box.

Panel de EC2

Vista global de EC2

Eventos

▼ Instancias

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamientos dedicados

Reservas de capacidad

Imágenes

AMI

Catálogo de AMI

▼ Elastic Block Store

Volumenes

Instancias

Administrador del ciclo de vida

▼ Red y seguridad

Security Groups

Direcciones IP elásticas

Grupos de ubicación

Dirección IPv6

Estado de la instancia

En ejecución

Nombre DNS de IP privada (solo IPv4)

Nombre DNS de IP pública (solo IPv4)

DNS de IPv4 pública

ec2-35-89-75-219.us-west-2.compute.amazonaws.com | dirección abierta

Direcciones IP elásticas

Hallazgo de AWS Compute Optimizer

Suscribirse a AWS Compute Optimizer para recibir recomendaciones | Más información

Nombre del grupo de Auto Scaling

ID de VPC

vpc-0512e421c51e7da2e (Lab VPC)

Direcciones IP privadas secundarias

ID de Outpost

▼ Interfaces de red (1) Información

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

`ec2-user`

Esto lo conectará a la instancia EC2.

The screenshot shows the AWS training and certification interface. On the left, there is a sidebar with the following sections:

- Introducción a a**
- Información del laboratorio**
 - 1 hora
 - Idiomas disponibles
 - Valoración
- Recursos**
 - PEM de par de claves de EC2
 - Descargar PEM
 - PPK de par de claves de EC2
 - Descargar PPK
 - LabRegion

In the center, a PuTTY terminal window is open, showing the following text:

```
35.89.75.219 - PuTTY
Unable to use certificate file "C:\Users\miguel iligaray\Downloads\Ec2KeyPair
-PPK.ppk" (PuTTY SSH-2 private key)
login as: ec2-user
```

On the right, a green box contains the text: "a estas instrucciones."

Below the terminal window, there are instructions for step 10:

- Select **Open** again.
- 9. Select **Yes**, to trust and con
- 10. When prompted **login as**, enter: `ec2-user` This will connect you to the EC2 instance.
- 11. Windows Users, skip ahead to the next task.

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.

```
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 ps -aux | grep -v root | sudo tee SharedFolder  
s/processes.csv  
tee: SharedFolders/processes.csv: No such file or directory  
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND  
rpc        1709  0.0  0.3  67256  3356 ?        Ss   07:22   0:00 /sbin/rpcbind -  
w  
dbus       1711  0.0  0.4  58248  4116 ?        Ss   07:22   0:00 /usr/bin/dbus-d  
aemon --system --address=systemd: --nofork --nopidfile --systemd-activation  
libstor+  1715  0.0  0.1  12628  1864 ?        Ss   07:22   0:00 /usr/bin/lsmc  
d  
chrony     1718  0.0  0.3 120184  3172 ?        S    07:22   0:00 /usr/sbin/chron  
yd -F 2  
rngd       1725  0.0  0.4  94224  4556 ?        Ss   07:22   0:00 /sbin/rngd -f -  
-fill-watermark=0 --exclude=jitter  
postfix    2154  0.0  0.6  90400  6736 ?        S    07:22   0:00 pickup -l -t un  
ix -u  
postfix    2155  0.0  0.6  90476  6640 ?        S    07:22   0:00 qmgr -l -t unix  
-u  
ec2-user   2404  0.0  0.4 150624  4524 ?        S    07:23   0:00 sshd: ec2-user@  
pts/0  
ec2-user   2405  0.0  0.4 124736  3988 pts/0    Ss   07:23   0:00 -bash  
[ec2-user@ip-10-0-10-130 ~]$
```

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 subprocessos 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 subprocessos 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.

```
ec2-user@ip-10-0-10-130:~  
top - 07:31:17 up 9 min, 1 user, load average: 0.00, 0.01, 0.00  
Tasks: 86 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 : 966816 total, 394712 free, 72120 used, 499984 buff/cache  
KiB Swap: 0 total, 0 free, 0 used. 752872 avail Mem  


| PID | USER | PR | NI  | VIRT   | RES  | SHR  | S | %CPU | %MEM | TIME+   | COMMAND     |
|-----|------|----|-----|--------|------|------|---|------|------|---------|-------------|
| 1   | root | 20 | 0   | 123512 | 5452 | 3968 | S | 0.0  | 0.6  | 0:01.32 | 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:+ |
| 5   | root | 20 | 0   | 0      | 0    | 0    | I | 0.0  | 0.0  | 0:00.06 | kworker/u4+ |
| 6   | root | 0  | -20 | 0      | 0    | 0    | I | 0.0  | 0.0  | 0:00.00 | mm_percpu_+ |
| 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  | 0:00.22 | migration/1 |
| 16  | root | 20 | 0   | 0      | 0    | 0    | S | 0.0  | 0.0  | 0:00.01 | ksoftirqd/1 |
| 18  | root | 0  | -20 | 0      | 0    | 0    | I | 0.0  | 0.0  | 0:00.00 | kworker/1:+ |
| 20  | root | 20 | 0   | 0      | 0    | 0    | S | 0.0  | 0.0  | 0:00.00 | kdevtmpfs   |


```

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 Entrar para ingresar al editor de texto predeterminado.

27. Prensas `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`

