

Ivan Castillo

## Administrar archivos de registro

### Objetivos

En este laboratorio usted:

- Revise el último registro y las salidas del registro seguro de la máquina Linux

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 page. 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 corner. The 'PuTTY Configuration' dialog box is open, showing the 'Connection' category. The 'Options controlling the connection' section has 'Seconds between keepalives (0 to turn off)' set to 30. The 'Low-level TCP connection options' section has 'Disable Nagle's algorithm (TCP\_NODELAY option)' checked. The 'Internet protocol version' section has 'Auto' selected. The 'Logical name of remote host' and 'Logical name of remote host (e.g. for SSH key lookup)' fields are empty. A 'Copied' tooltip is visible over the '30' value in the 'Seconds between keepalives' field.

The screenshot shows the AWS Management Console. The left sidebar contains the 'Servicios' menu with categories like 'Panel de EC2', 'Instancias', 'Imágenes', 'Elastic Block Store', 'Volumenes', 'Administrador del ciclo de vida', 'Red y seguridad', and 'Grupos de ubicación'. The main content area shows the 'Detalles de red' section for an EC2 instance. The 'Dirección IPv4 pública' is '35.89.75.219' with a link to 'dirección abierta'. The 'Dirección IP asignada automáticamente' is 'ip-10-0-10-77.us-west-2.compute.internal'. The 'Dirección IP privada (solo IPv4)' is 'ip-10-0-10-77.us-west-2.compute.internal'. The 'Dirección IP elástica' is 'ec2-35-89-75-219.us-west-2.compute.amazonaws.com' with a link to 'dirección abierta'. The 'Direcciones IP elásticas' section shows 'vpc-0512e421c51e7da2e (Lab VPC)' with a link to 'Más información'. The 'ID de VPC' is 'vpc-0512e421c51e7da2e (Lab VPC)' with a link to 'Más información'. The 'ID de Outpost' is 'id-0512e421c51e7da2e (Lab Outpost)' with a link to 'Más información'. The 'PuTTY Configuration' dialog box is open, showing the 'Basic options for your PuTTY session' section. The 'Host (Name or IP address)' field is '35.89.75.219'. The 'Port' field is '22'. The 'Connection type' is 'SSH'. The 'Load, save or delete a stored session' section has 'Save' and 'Delete' buttons. The 'Close window on exit' section has 'Always' and 'Only on clean exit' options. A 'Copied' tooltip is visible over the '35.89.75.219' value in the 'Host' field.

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.

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 is a list of instructions:

- 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: revisar archivos de registro seguros

En esta tarea, utilizará herramientas comunes de Linux para revisar los archivos de registro **seguros** y utilizará la aplicación **Lastlog** de Linux para revisar los inicios de sesión anteriores.

18. Para validar que estás en la carpeta de inicio **de la empresaA** , ingresa `pwd` y presione Entrar.

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

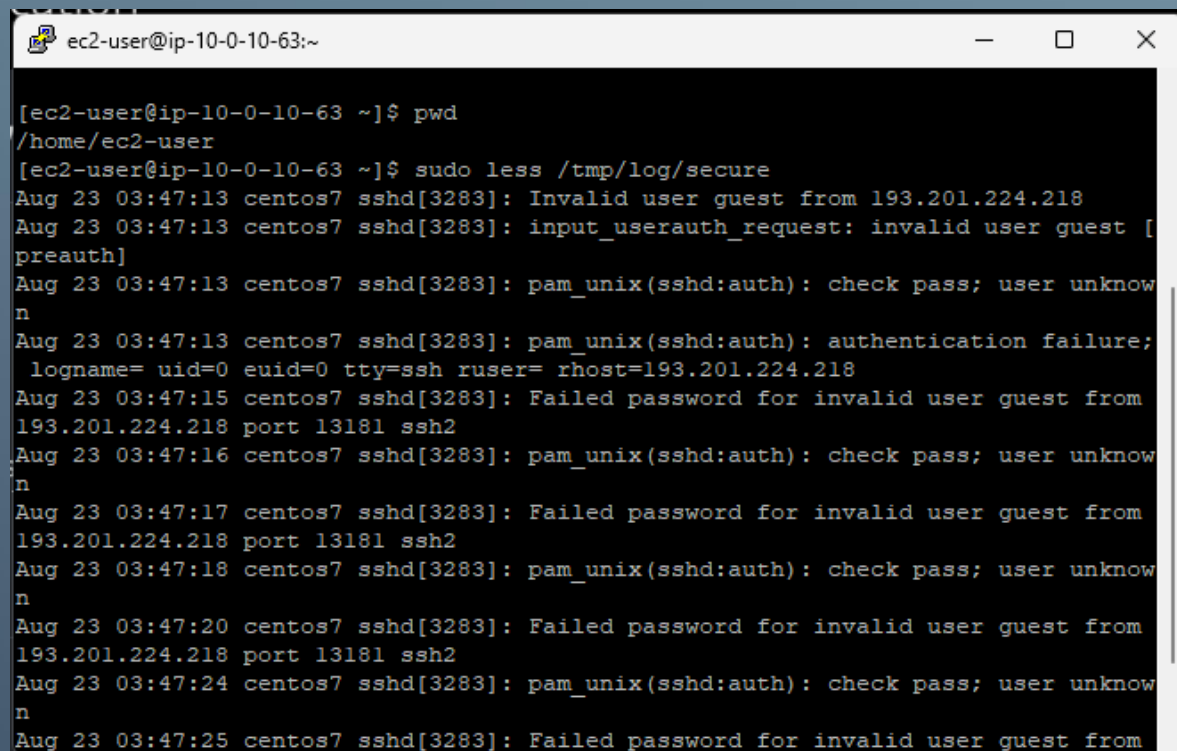
19. Para utilizar el archivo de registro seguro como prueba, ingrese `sudo less /tmp/log/secure` y presione Entrar.

### Nota

Normalmente, el archivo de registro seguro se encuentra en `/var/log/secure` . Esta práctica de laboratorio presenta un archivo de registro seguro de muestra en `/tmp/log/secure` .

20. Para salir del programa, ingrese `q`

21. Para ver las últimas horas de inicio de sesión de todos los usuarios de la máquina, ingrese `sudo lastlog` y presione Entrar.



```
ec2-user@ip-10-0-10-63:~  
[ec2-user@ip-10-0-10-63 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-10-0-10-63 ~]$ sudo less /tmp/log/secure  
Aug 23 03:47:13 centos7 sshd[3283]: Invalid user guest from 193.201.224.218  
Aug 23 03:47:13 centos7 sshd[3283]: input_userauth_request: invalid user guest [  
preauth]  
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow  
n  
Aug 23 03:47:13 centos7 sshd[3283]: pam_unix(sshd:auth): authentication failure;  
  logname= uid=0 euid=0 tty=ssh ruser= rhost=193.201.224.218  
Aug 23 03:47:15 centos7 sshd[3283]: Failed password for invalid user guest from  
193.201.224.218 port 13181 ssh2  
Aug 23 03:47:16 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow  
n  
Aug 23 03:47:17 centos7 sshd[3283]: Failed password for invalid user guest from  
193.201.224.218 port 13181 ssh2  
Aug 23 03:47:18 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow  
n  
Aug 23 03:47:20 centos7 sshd[3283]: Failed password for invalid user guest from  
193.201.224.218 port 13181 ssh2  
Aug 23 03:47:24 centos7 sshd[3283]: pam_unix(sshd:auth): check pass; user unknow  
n  
Aug 23 03:47:25 centos7 sshd[3283]: Failed password for invalid user guest from
```

```
ec2-user@ip-10-0-10-63:~  
systemd-network      **Never logged in**  
dbus                  **Never logged in**  
rpc                   **Never logged in**  
libstoragemgmt        **Never logged in**  
sshd                  **Never logged in**  
rngd                  **Never logged in**  
chrony                **Never logged in**  
rpcuser               **Never logged in**  
nfsnobody             **Never logged in**  
ec2-instance-connect  **Never logged in**  
postfix               **Never logged in**  
tcpdump               **Never logged in**  
ec2-user      pts/0    201.189.202.99  Wed Jan  3 09:47:21 +0000 2024  
ljuan                 **Never logged in**  
mmajor                **Never logged in**  
mjackson              **Never logged in**  
eowusu                **Never logged in**  
nwolf                 **Never logged in**  
arosalez              **Never logged in**  
jdoe                  **Never logged in**  
psantos               **Never logged in**  
smartinez             **Never logged in**  
ssarkar               **Never logged in**  
[ec2-user@ip-10-0-10-63 ~]$
```