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

Estasinstruccionessonespecíficamente parausuarios de Windows. Si estáutilizando macOS o Linux, pase a la siguiente sección.

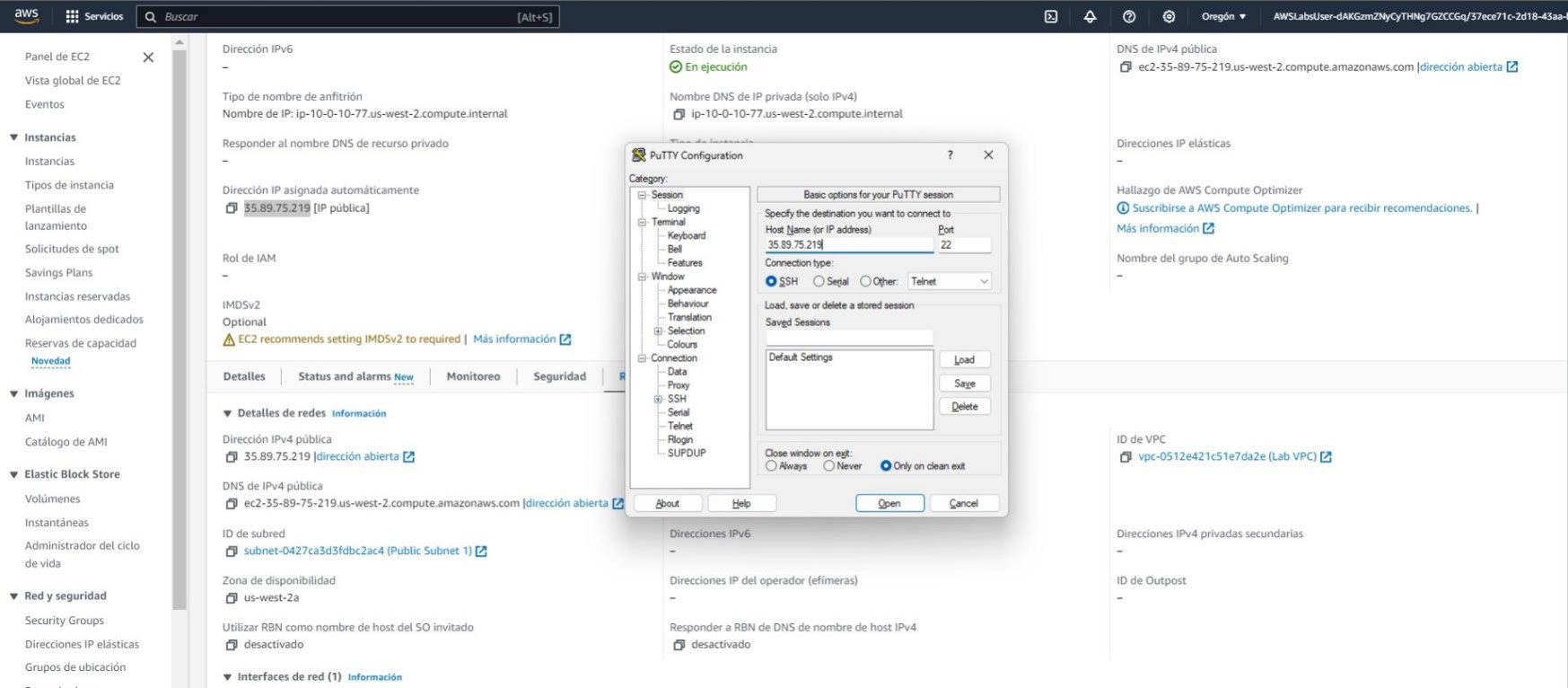
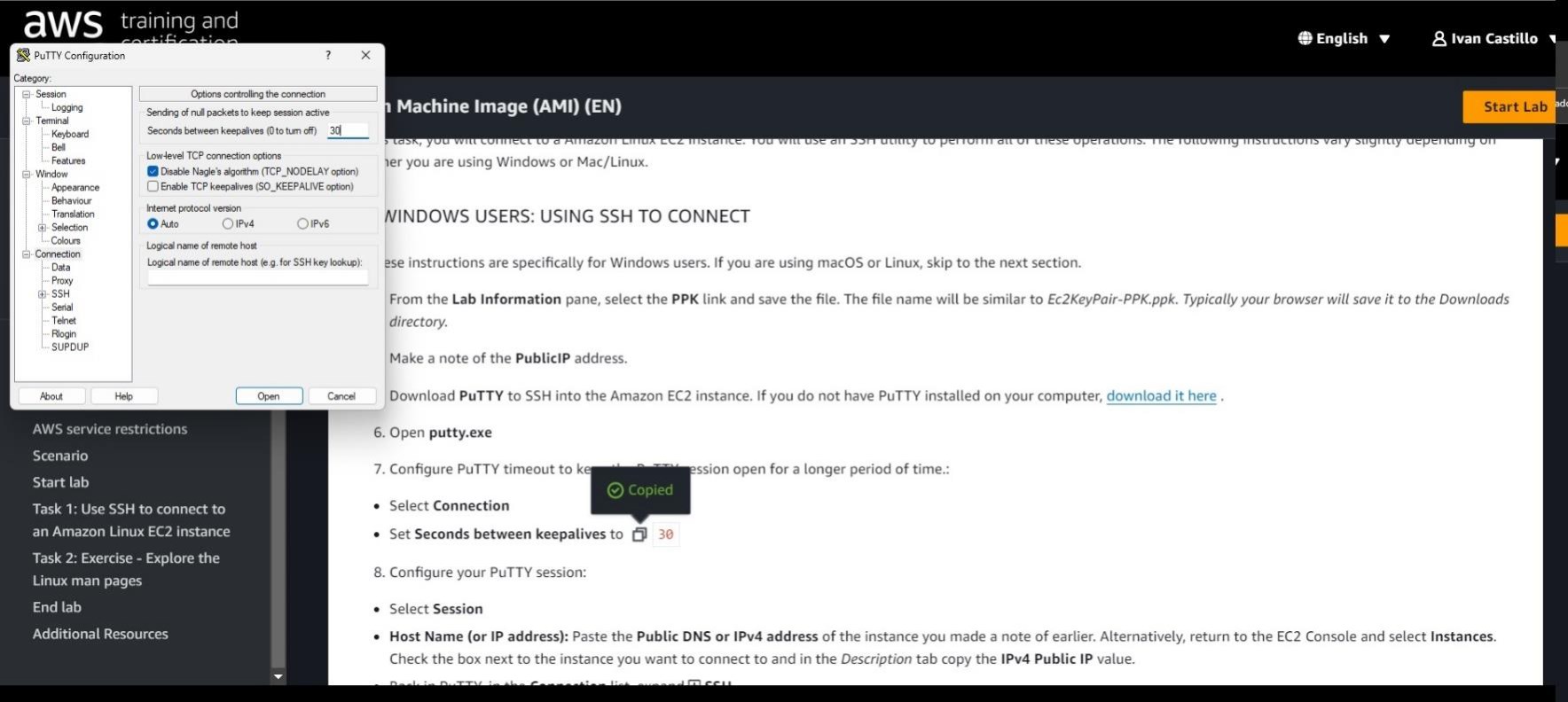
3. En el panel **Información del laboratorio** , seleccione el enlace **PPK** y guarde el archivo. El nombre del archivo será similar a *Ec2KeyPair-PPK.ppk* . *Normalmente su navegador lo guardará en el directorio de Descargas.*

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**

· Establecer **segundos entre keepalives** en 30

8. Configure su sesión PuTTY:

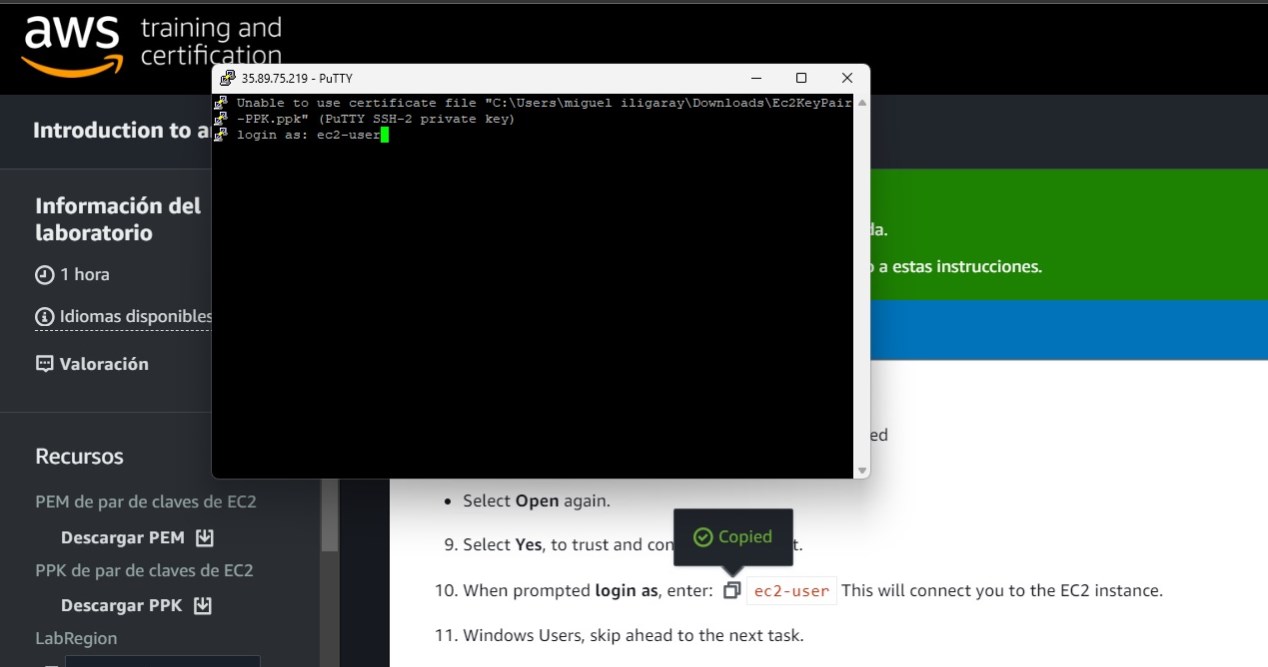
· Seleccionar **sesión**

· **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** .

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

ec2-user

 Esto lo conectará a la instancia EC2.



**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.

1. 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.

1. 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** .

1. Para salir del programa, ingrese q
2. Para ver las últimas horas de inicio de sesión de todos los usuarios de la máquina, ingrese sudo lastlog y presione Entrar.

