Ivan Castillo

S5: Laboratorio: Comandos de solución de problemas del protocolo de Internet

Objetivos

En este laboratorio usted:

* Practicar los comandos de solución de problemas
* Identificar cómo puede usar estos comandos en las situaciones del cliente

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

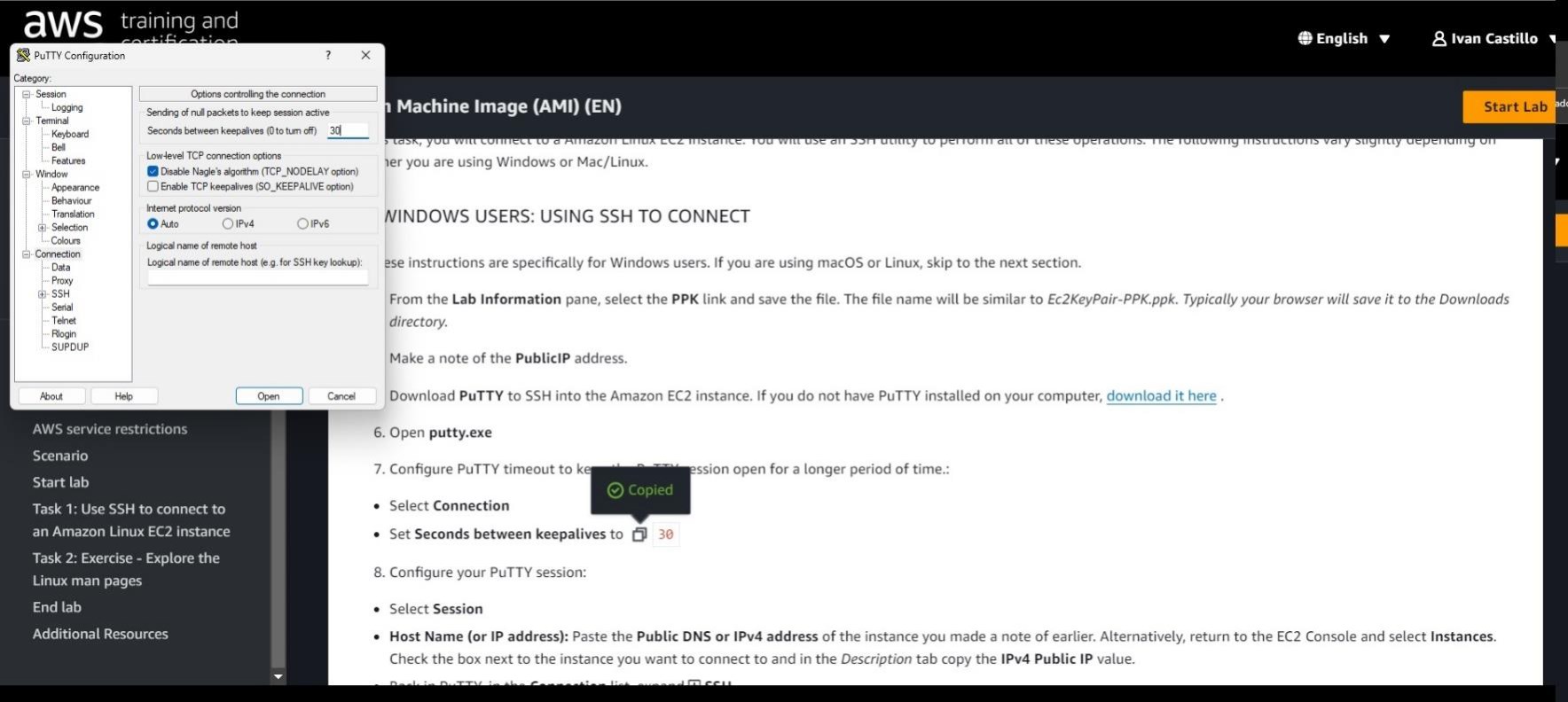
Estasinstruccionessonespecíficamente parausuarios de Windows. Si estáutilizando macOS o Linux, pase a la siguiente sección.

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:

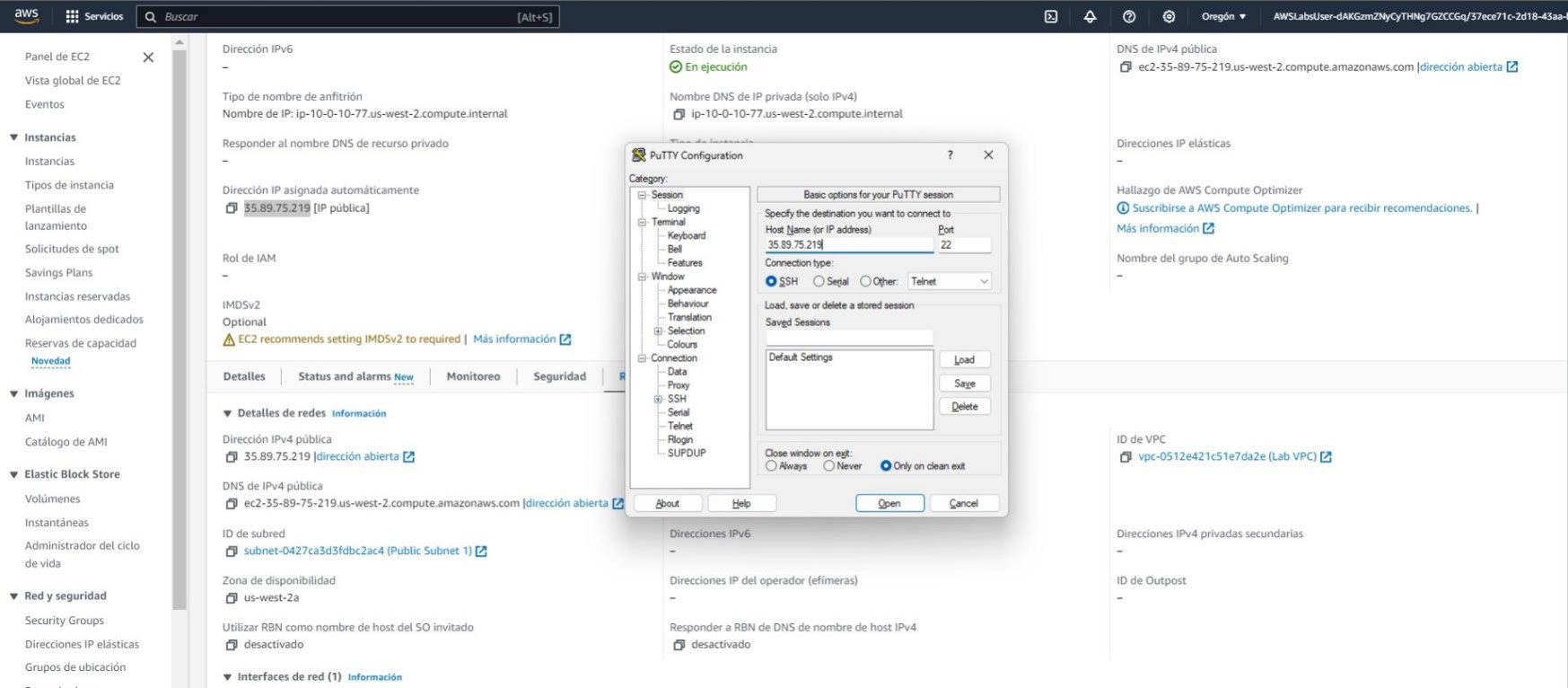
· Seleccionar **conexión**

· 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.

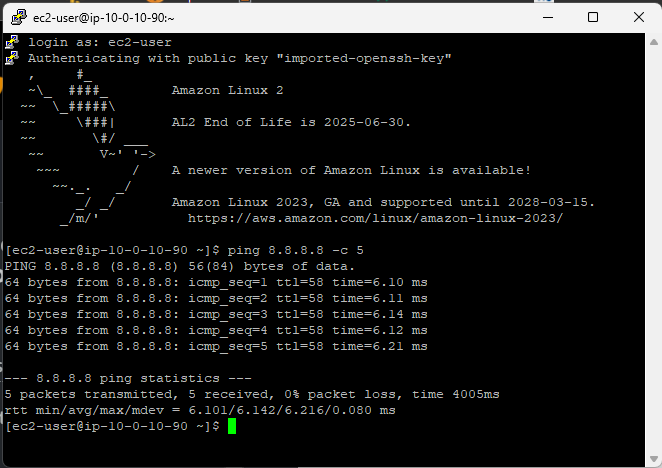
**Tarea 2: Practicar los comandos de solución de problemas**

1. El siguiente es un ejemplo de una situación de cliente en el que puede usar el comando ping:

El cliente ha lanzado una instancia de EC2. Para probar la conectividad hacia y desde la instancia, ejecute el comando ping. Puede usar este comando para probar la conectividad y asegurarse de que permite las solicitudes del Protocolo de mensajes de control de Internet (ICMP) en el nivel de seguridad, como grupos de seguridad y ACL de red.

En la terminal de Linux, ejecute el siguiente comando y presione Enter:

ping 8.8.8.8 -c 5

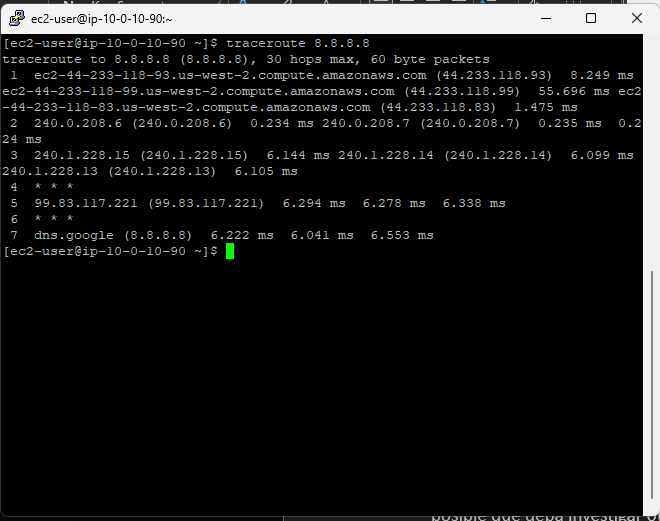


1. ****El siguiente es un ejemplo de una situación de cliente en el que puede usar el comando traceroute:

El cliente tiene problemas de latencia. Dice que su conexión tarda mucho y que pierde paquetes. No está seguro de si está relacionado con AWS o con su proveedor de servicios de Internet (ISP). Para investigar, puede ejecutar el comando traceroute desde su recurso de AWS al servidor al que intentan acceder. Si la pérdida ocurre hacia el servidor, lo más probable es que el problema sea el ISP. Si la pérdida es para AWS, es posible que deba investigar otros factores que pudieran limitar la conectividad de red.

En la terminal de Linux, ejecute el siguiente comando y presione Enter:

traceroute 8.8.8.8

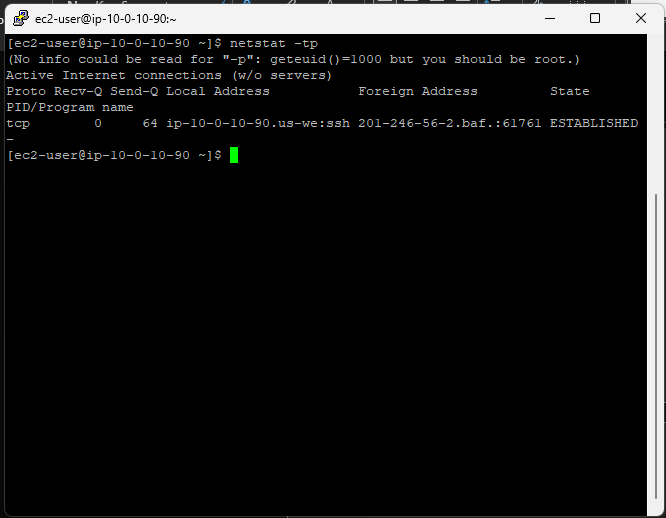


1. ****El siguiente es un ejemplo de una situación de cliente donde puede usar el comando netstat:

La empresa ejecuta un análisis de seguridad de rutina y descubrió que se ha puesto en riesgo uno de los puertos en una determinada subred. Para confirmar, ejecute el comando netstat en un host local en esa subred para confirmar si el puerto escucha cuando no debería hacerlo.

En la terminal de Linux, ejecute el siguiente comando y presione Enter:

netstat -tp



1. ****El siguiente es un ejemplo de una situación de cliente donde puede usar el comando telnet:

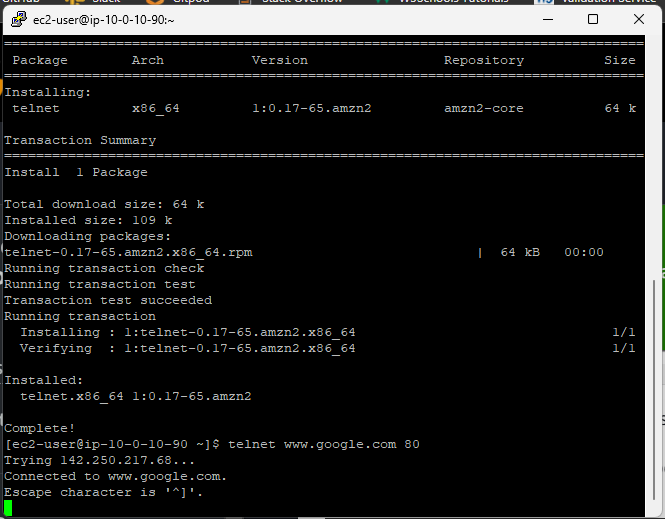
El cliente tiene un servidor web seguro y tiene configuradas reglas de grupo de seguridad personalizadas y reglas de ACL de red. Sin embargo, les preocupa que el puerto 80 esté abierto a pesar de que muestra que su configuración de seguridad indica que su grupo de seguridad bloque este puerto, puede ejecutar el comando telnet 192.168.10.5 80 para asegurarse de que se rechace la conexión.

En la terminal de Linux, ejecute el siguiente comando y presione Enter para instalar telnet:

sudo yum install telnet -y

En la terminal de Linux, ejecute el siguiente comando y presione Enter:

telnet www.google.com 80



1. ****El siguiente es un ejemplo de una situación del cliente en el que puede usar el comando curl:

El cliente tiene un servidor Apache ejecutándose y quiere probar si está recibiendo una solicitud exitosa (200 OK), lo que indica que su sitio web se está ejecutando de manera correcta. Puede ejecutar una solicitud del comando curl para ver si el servidor Apache del cliente devuelve una respuesta 200 OK.

En la terminal de Linux, ejecute el siguiente comando y presione Enter:

curl -vLo /dev/null <https://aws.com>

