Usar SSH y SCP con el Administrador de Sesión de AWS para Conectarse a una instancia EC2

Para mejorar la seguridad de la conexión y acceso a las instancias EC2, muchas veces se utiliza el Administrador de Sesión (SSM) de AWS y se elimina el uso de IPs públicas/privadas para exponer dichas instancias y así poder conectarse a ellas. La conexión se establece utilizando la línea de comandos de SSM.

Pero, ¿que pasa si necesitas enviar archivos a la instancia? Usualmente se haría usando SCP, pero si no tenemos una dirección para la instancia, entonces, ¿cómo podemos hacerlo?

Bueno, a continuación te explico qué hacer para poder habilitar el uso de SSH y SCP en nuestro sistema.

# Pre-requisitos

* Instalar:
  + AWS CLI (configurar por lo menos el nombre de la región. Ej.: us-west-2)
  + Session Manager Plugin
* Contar el archivo PEM de la instancia

# Habilitar la conexión

## En Windows

### Ajustes en la configuración de SSH

El cliente de OpenSSH está disponible como un componente instalable en las versiones más recientes de windows. Para más información sobre cómo instalarlo, visita [Cómo instalar OpenSSH](https://docs.microsoft.com/en-us/windows-server/administration/openssh/openssh_install_firstuse).

Normalmente encontrarás el archivo de configuración de SSH en C:\Users\{username}\.ssh\config. Sin embargo, el directorio .ssh no existirá hasta que ssh sea usado.

Agrega lo siguiente al archivo de configuración:

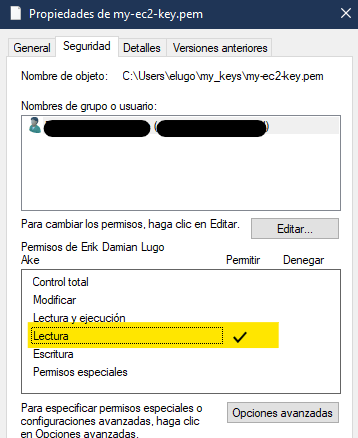
# SSH over Session Manager

host i-\* mi-\*

ProxyCommand C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters portNumber=%p"

### Permisos del archivo PEM

El archivo pem deberá tener propiedades de acceso de sólo lectura, para el usuario que inició sesión en el sistema. Para esto, utililza las opciones avanzadas de Seguridad, en las propiedades del archivo:



## En Linux

### Ajustes en la configuración de SSH

El archivo de configuración se encuentra en ~/.ssh/config. Edita este archivo y agrega lo siguiente:

# SSH over Session Manager

host i-\* mi-\*

ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters 'portNumber=%p'"

### Permisos del archivo PEM

El archivo pem deberá tener propiedades de acceso de sólo lectura, para el usuario que inició sesión en el sistema. Para esto, ejecuta la siguietne instrucción:

chmod 400 my\_key.pem

# Conectémonos

Ahora que hemos realizado los ajustes necesarios, ya podremos utilizar SSH y SCP.

**Establecer conexión con la instancia (SSH)**

ssh -i key.pem nombre\_usuario@id\_instancia -p XX

**Subir un archivo (SCP)**

scp -i key.pem some\_bugfix.zip nombre\_usuario@id\_instancia:/remote\_dir/some\_bugfix.zip

# Fuentes

El artículo original se puede consultar en [Using AWS Session Manager with Enhanced SSH and SCP Capability](https://www.tripwire.com/state-of-security/security-data-protection/cloud/aws-session-manager-enhanced-ssh-scp-capability/).