

# Conectarse a la instancia de Linux desde Windows mediante PuTTY

[PDF \(ec2-ug.pdf#putty\)](#) | [RSS \(amazon-ec2-release-notes.rss\)](#)

Si ejecuta Windows Server 2019 o posterior, le recomendamos usar OpenSSH, que es una herramienta de conectividad de código abierto para iniciar sesión de forma remota con el protocolo SSH. Para obtener información sobre los pasos para conectarse a una instancia de Linux desde Windows mediante OpenSSH, consulte [Conectarse a la instancia de Linux desde Windows mediante OpenSSH \(./openssh.html\)](#) .

Las siguientes instrucciones explican cómo conectarse a la instancia mediante PuTTY, un cliente SSH para Windows. Si aparece un error al intentar conectarse a la instancia, consulte [Solucione el problema de conectar la instancia. \(./TroubleshootingInstancesConnecting.html\)](#) .

## Contenido

- [Requisitos previos \(./putty.html#putty-prereqs\)](#)
  - [Convierta su clave privada utilizando PuTTYgen \(./putty.html#putty-private-key\)](#)
- [Conexión con la instancia de Linux \(./putty.html#putty-ssh\)](#)
- [Transferir archivos a la instancia de Linux mediante el cliente Secure Copy de PuTTY \(./putty.html#putty-scp\)](#)
- [Transferir archivos de la instancia de Linux mediante WinSCP \(./putty.html#Transfer\\_WinSCP\)](#)

---

## Requisitos previos

Antes de conectarse a la instancia de Linux mediante PuTTY, se deben completar los siguientes requisitos previos:


### Verifique que la instancia está lista

Una vez lanzada la instancia, pueden transcurrir unos minutos hasta que esté lista para conectarse. Verifique que su instancia ha pasado las comprobaciones de estado. Puede ver esta información en la columna **Status check (Comprobación de estado)** de la página **Instances** (Instancia[s]).

### Verifique los requisitos previos generales para conectarse a la instancia

Para encontrar el nombre de DNS público o la dirección IP de la instancia y el nombre de usuario que debería utilizar para conectarse a la instancia, consulte [Configuración para conectarse a la instancia \(./connection-prereqs.html\)](#) .

## Instale PuTTY en su equipo local

Descargue e instale PuTTY desde la [página de descarga de PuTTY](http://www.chiark.greenend.org.uk/~sgtatham/putty/) 

(<http://www.chiark.greenend.org.uk/~sgtatham/putty/>) . Si ya tiene instalada una versión antigua de PuTTY, le recomendamos que descargue la última versión. Asegúrese de instalar el conjunto completo.

## Convierta su clave .pem privada en .ppk con PuTTYgen

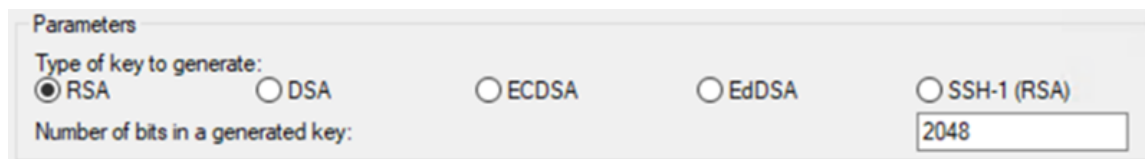
Para el par de claves especificado al lanzar la instancia, si eligió crear la clave privada en formato .pem, debe convertirla en un archivo .ppk para usarla con PuTTY. Busque el archivo .pem privado y, a continuación, siga los pasos que se indican en la siguiente sección.

## Convierta su clave privada utilizando PuTTYgen

PuTTY no admite de forma nativa el formato PEM para claves SSH. PuTTY proporciona una herramienta llamada PuTTYgen, la cual convierte claves al formato requerido PPK para PuTTY. Debe convertir su clave privada (archivo .pem) a este formato (archivo .ppk) como se indica a continuación para conectarse a la instancia mediante PuTTY.

### Para convertir una clave .pem privada al formato .ppk

1. En el menú **Start (Inicio)**, elija **All Programs (Todos los programas)**, **PuTTY**, **PuTTYgen**.
2. En **Type of key to generate (Tipo de clave a generar)**, elija **RSA**. Si la versión de PuTTYgen no incluye esta opción, elija **SSH-2 RSA**.



Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key:

3. Elija **Load (Cargar)**. De forma predeterminada, PuTTYgen muestra solo archivos con la extensión .ppk . Para localizar el archivo .pem , seleccione la opción de mostrar todos los tipos de archivo.



File name:

PuTTY Private Key Files (\*.ppk)

PuTTY Private Key Files (\*.ppk)

All Files (\*.\*)

4. Seleccione el archivo .pem para el par de claves que especificó cuando lanzó la instancia y, a continuación, elija **Open (Abrir)**. PuTTYgen muestra un aviso de que el archivo .pem se ha importado correctamente. Seleccione **OK**.
5. Elija **Save private key** (Guardar la clave privada) para guardar la clave en formato que PuTTY pueda utilizar. PuTTYgen mostrará una advertencia acerca de guardar la clave sin una frase de contraseña. Elija **Yes (Sí)**.

### **nota**

Una contraseña de una clave privada es una capa adicional de protección. Incluso si se descubriera su clave privada, no se puede usar sin la contraseña. El inconveniente de usar una contraseña es que dificulta la automatización puesto que la intervención humana es necesaria para iniciar una sesión en una instancia o para copiar archivos en una instancia.

6. Especifique el mismo nombre para la clave que utilizó para el par de claves (por ejemplo `key-pair-name`) y elija **Save** (Guardar). PuTTY añade la extensión de archivo `.ppk` automáticamente.

La clave privada está ahora en el formato correcto para su uso con PuTTY. Ya puede conectarse a la instancia mediante el cliente SSH de PuTTY.

## Conexión con la instancia de Linux

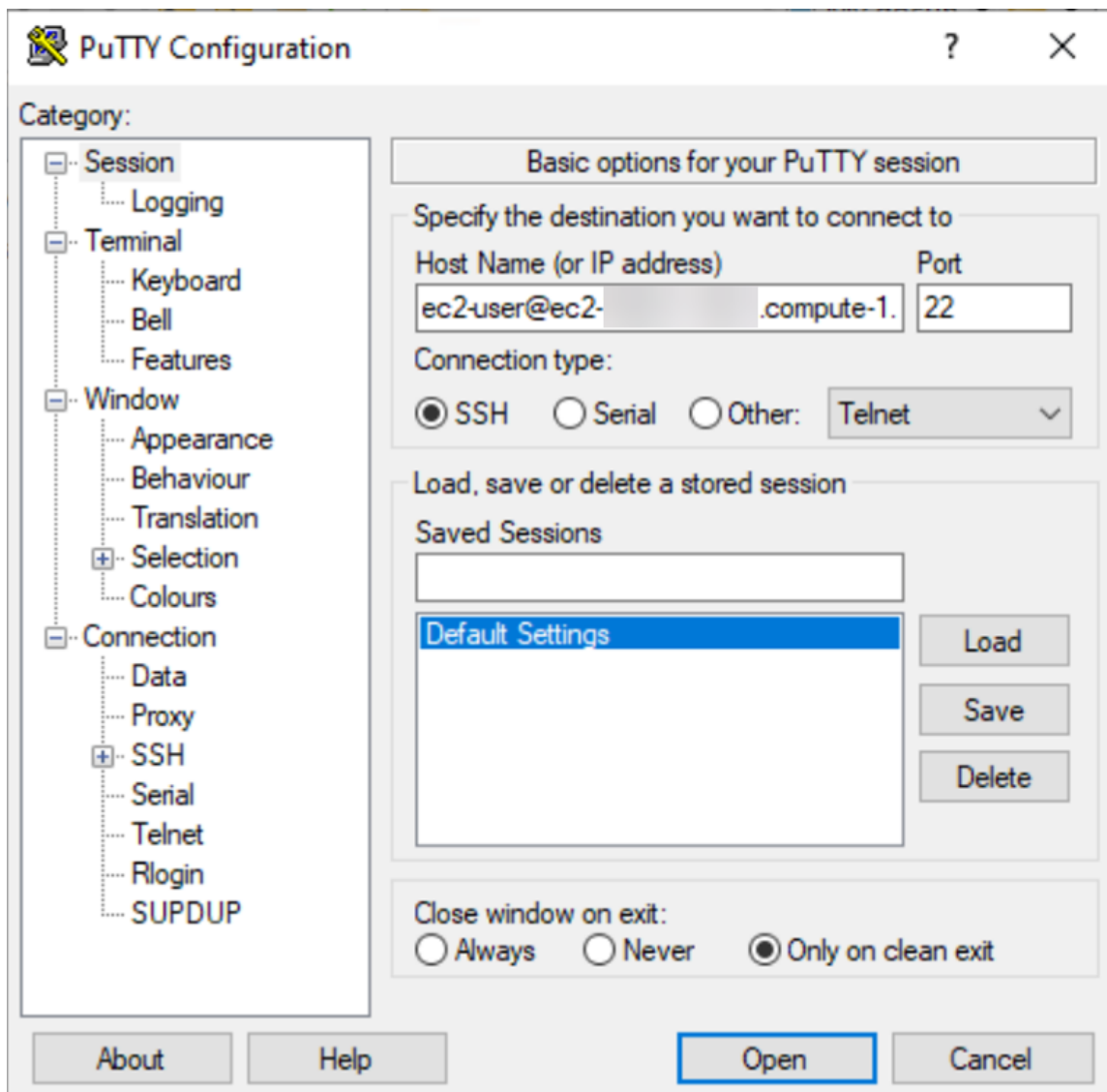
Para conectarse a la instancia de Linux mediante PuTTY, use el siguiente procedimiento. Necesita el archivo `.ppk` que creó para la clave privada. Para obtener más información, consulte [Convierta su clave privada utilizando PuTTYgen \(#putty-private-key\)](#) en la sección anterior. Si aparece un error al intentar conectarse a la instancia, consulte [Solucione el problema de conectar la instancia. \(/TroubleshootingInstancesConnecting.html\)](#).

### Para conectarse a la instancia mediante PuTTY

1. Inicie PuTTY (en el menú **Inicio**, elija **Todos los programas, PuTTY, PuTTY**).
2. En el panel **Category (Categoría)**, elija **Session (Sesión)** y rellene los siguientes campos:
  - a. En el cuadro **Host Name (Nombre de host)** siga uno de estos procedimientos:
    - (DNS público) Para conectarse utilizando el nombre DNS público de la instancia, escriba `instance-user-name @ instance-public-dns-name`.
    - (IPv6) Como opción, si la instancia tiene una dirección IPv6, para conectarse utilizando esta dirección IPv6, escriba `instance-user-name @ instance-IPv6-address`.

Para obtener información acerca de cómo obtener el nombre de usuario de la instancia y el nombre de DNS público o la dirección IPv6 de la instancia, consulte [Obtenga información sobre su instancia \(/connection-prereqs.html#connection-prereqs-get-info-about-instance\)](#).

- b. Asegúrese de que el valor del **Port (Puerto)** es 22.
- c. En **Connection type (Tipo de conexión)**, seleccione **SSH**.



3. (Opcional) Puede configurar PuTTY para que envíe datos "keepalive" a intervalos regulares para mantener la sesión activa. Esto es útil para evitar desconectarse de su instancia por inactividad en la sesión. En el panel **Category (Categoría)**, elija **Connection (Conexión)** y escriba el intervalo deseado en el campo **Seconds between keepalives (Segundos entre keepalives)**. Por ejemplo, si su sesión se desconecta tras 10 minutos de inactividad, escriba 180 para que PuTTY envíe datos "keepalive" cada 3 minutos.
4. En el panel **Categoría**, expanda **Conexión**, **SSH** y **Autenticación**, luego elija **Credenciales**. Haga lo siguiente:
  - a. Junto a **Archivo de clave privada para la autenticación**, selecciona **Examinar**.
  - b. Seleccione el archivo .ppk que ha generado para su par de claves y elija **Open (Abrir)**.
  - c. (Opcional) Si tiene previsto volver a iniciar esta sesión más adelante, puede guardar la sesión informativa para usarla en el futuro. En **Category (Categoría)**, elija **Session (Sesión)**, escriba un nombre para la sesión en **Saved Sessions (Sesiones guardadas)** y, a continuación, elija **Save (Guardar)**.
  - d. Elija **Open**.

5. Si esta es la primera vez que se conecta a esta instancia, PuTTY muestra un cuadro de diálogo de alerta de seguridad que le pregunta si tiene confianza en el host al que se está conectando.
  - a. (Opcional) Verifique que la huella digital en el cuadro de diálogo de la alerta de seguridad coincide con la huella digital que obtuvo anteriormente en [\(Opcional\) Obtenga la huella digital de la instancia \(/connection-prereqs.html#connection-prereqs-fingerprint\)](#) . Si estas huellas digitales no coinciden, alguien podría intentar un ataque man-in-the-middle (MITM). Si coinciden, continúe con el siguiente paso.
  - b. Elija **Accept (Aceptar)**. Se abre una ventana y está conectado a la instancia.

**📌 nota**

Si especificó una frase de contraseña al convertir la clave privada al formato PuTTY, deberá indicar la contraseña cuando inicie sesión en la instancia.

Si aparece un error al intentar conectarse a la instancia, consulte [Solucione el problema de conectar la instancia. \(/TroubleshootingInstancesConnecting.html\)](#) .

## Transferir archivos a la instancia de Linux mediante el cliente Secure Copy de PuTTY

El cliente Secure Copy de PuTTY (PSCP) es una herramienta de línea de comandos que puede usar para transferir archivos entre el equipo Windows y la instancia de Linux. Si prefiere una interfaz de usuario gráfica (GUI), puede usar una herramienta de GUI de código abierto llamada WinSCP. Para obtener más información, consulte [Transferir archivos de la instancia de Linux mediante WinSCP \(#Transfer\\_WinSCP\)](#) .

Para usar PSCP, necesita la clave privada que generó en [Convierta su clave privada utilizando PuTTYgen \(#putty-private-key\)](#) . También necesita el nombre de DNS público de su instancia de Linux o la dirección IPv6 si su instancia tiene una.

El siguiente ejemplo transfiere el archivo `Sample_file.txt` desde la unidad `C:\` de un equipo Windows al directorio principal `instance-user-name` de una instancia de Amazon Linux: Para transferir un archivo, utilice uno de los siguientes comandos.

- (DNS público) Para transferir un archivo utilizando el nombre DNS público de la instancia, escriba el siguiente comando.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) Como opción, si la instancia tiene una dirección IPv6, para transferir un archivo utilizando la dirección IPv6 de su instancia, escriba el siguiente comando. La dirección IPv6 se debe escribir entre

corchetes ( [ ] ).

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-  
name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```


## Transferir archivos de la instancia de Linux mediante WinSCP

WinSCP es un administrador de archivos basado en GUI para Windows que le permite cargar y transferir archivos a un equipo remoto mediante los protocolos SFTP, SCP, FTP y FTPS. WinSCP le permite arrastrar y soltar archivos desde el equipo con Windows a la instancia de Linux, o sincronizar estructuras de directorios completas entre los dos sistemas.

### Requisitos

- Debe tener la clave privada que se generó en [Convierta su clave privada utilizando PuTTYgen \(#putty-private-key\)](#) .
- También necesita el nombre DNS público de la instancia de Linux.
- La instancia de Linux debe tener instalado `scp` . En algunos sistemas operativos, puede instalar el paquete `openssh-clients` . En otros, como la AMI optimizada para Amazon ECS, puede instalar el paquete `scp` . Compruebe la documentación de su distribución Linux.

### Para conectarse a la instancia mediante WinSCP

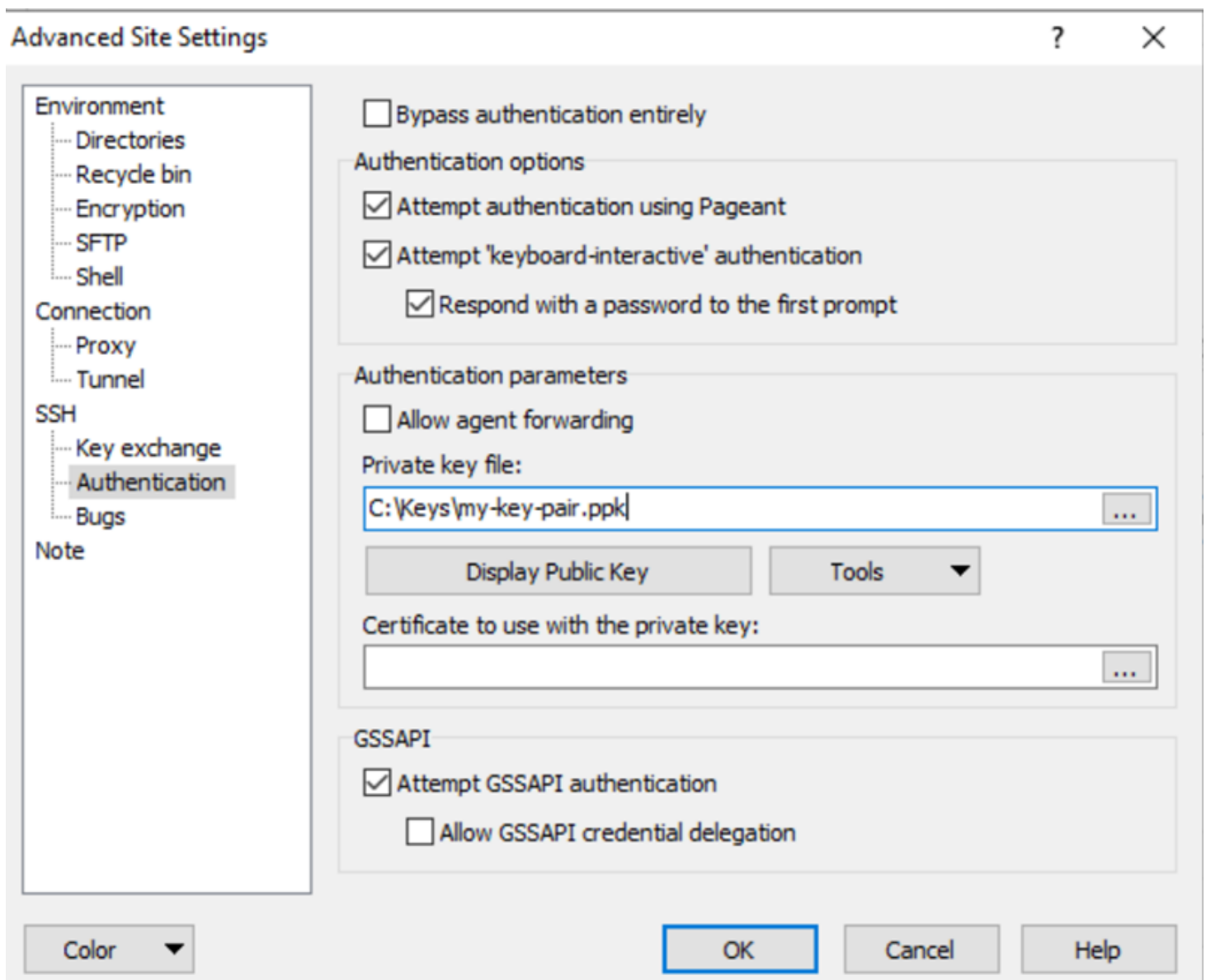
1. Descargue e instale WinSCP desde <http://winscp.net/eng/download.php>  (<http://winscp.net/eng/download.php>) . La mayoría de usuarios no necesitará modificar las opciones de instalación predeterminadas.
2. Inicie WinSCP.
3. En la pantalla **inicio de sesión de WinSCP** en **Nombre de host**, escriba una de las siguientes opciones:
  - (DNS público o dirección IPv4) Para iniciar sesión con el nombre de DNS público o la dirección IPv4 pública de la instancia, introduzca el nombre de DNS público o la dirección IPv4 pública de la instancia.
  - (IPv6) Como opción, si la instancia tiene una dirección IPv6, para iniciar sesión utilizando la dirección IPv6 de la instancia, escriba la dirección IPv6 de la instancia.
4. En **User name (Nombre de usuario)**, escriba el nombre de usuario predeterminado para la AMI.
  - En el caso de Amazon Linux 2023, Amazon Linux 2 o la AMI de Amazon Linux, el nombre de usuario es `ec2-user` .
  - Para una AMI de CentOS, el nombre de usuario es `centos` o `ec2-user` .
  - Para una AMI de Debian, el nombre de usuario es `admin` .
  - Para una AMI de Fedora, el nombre de usuario es `fedora` o `ec2-user` .
  - Para una AMI de RHEL, el nombre de usuario es `ec2-user` o `root` .

- Para una AMI de SUSE, el nombre de usuario es `ec2-user` o `root`.
- Para una AMI de Ubuntu, el nombre de usuario es `ubuntu`.
- Para una AMI de Oracle, el nombre de usuario es `ec2-user`.
- Para una AMI de Bitnami, el nombre de usuario es `bitnami`.
- De lo contrario, verifíquelo con el proveedor de AMI.

5. Especifique la clave privada de la instancia.

- Elija la opción **Avanzado...** botón.
- En SSH, selecciona **Autenticación**.
- Especifique la ruta del archivo de clave privada o elija la... botón para buscar el archivo del key pair.
- Seleccione **OK (Aceptar)**.

Aquí hay una captura de pantalla de WinSCP versión 6.1:

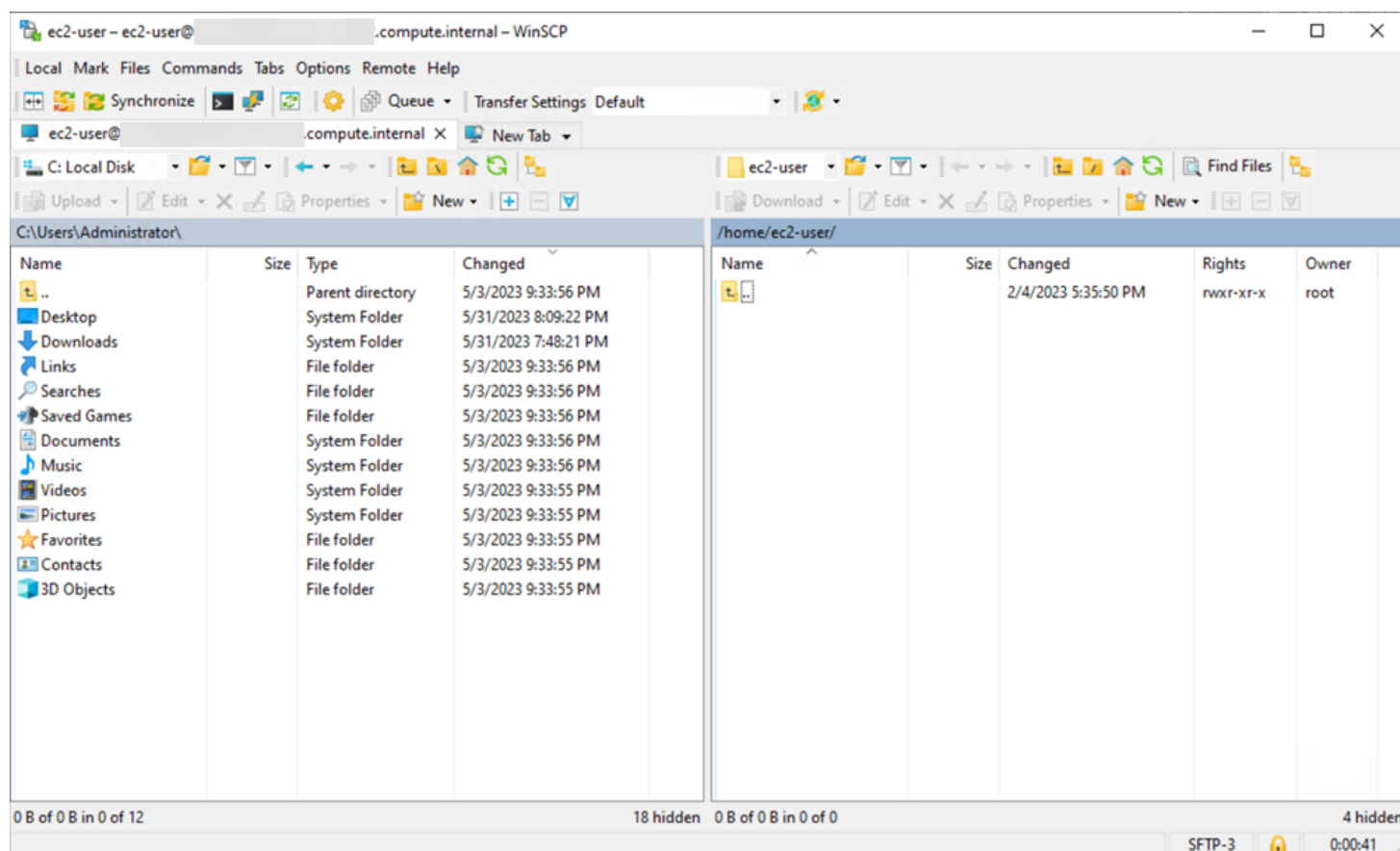


WinSCP requiere un archivo () de clave privada de Pu ( .ppk ). Puede convertir un archivo de clave de seguridad .pem en el formato .ppk mediante PuTTYgen. Para obtener más información, consulte



Convierta su clave privada utilizando PuTTYgen (#putty-private-key) .

- De forma opcional, en el panel izquierdo, elija **Directories (Directorios)**. En **Remote directory (Directorio remoto)**, introduzca la ruta del directorio al que se añaden los archivos. Para abrir la configuración avanzada, para las versiones más recientes de WinSCP, elija **Advanced (Avanzada)**. Para encontrar la configuración del **Remote directory (Directorio remoto)**, en **Environment (Entorno)**, elija **Directories (Directorios)**.
- Seleccione **Login (Iniciar sesión)**. Para añadir la huella digital del host a la caché del host, elija **Yes (Sí)**.



- Una vez establecida la conexión, la instancia de Linux aparece a la derecha y el equipo local a la izquierda en la ventana de conexión. Puede arrastrar y soltar archivos entre el sistema de archivos remoto y la máquina local. Para obtener más información sobre WinSCP, consulte la documentación del proyecto en <http://winscp.net/eng/docs/start> .

Si recibe un error que indica que no puede ejecutar SCP para iniciar la transferencia, compruebe que **scp** esté instalado en la instancia de Linux.