

Acceso a la CLI de AMP para nube privada a través de SSH y transferencia de archivos a través de SCP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Generar un par de claves RSA mediante PuTTY](#)

[Genere un par de llaves RSA usando Linux/Mac](#)

[Adición de las claves públicas generadas al portal de administración de AMP para nube privada](#)

[Utilice el par de claves generado para SSH en el dispositivo mediante PuTTY](#)

[Uso del par de claves configurado para SSH en el dispositivo mediante Linux](#)

[Uso de WinSCP para interactuar con el sistema de archivos de AMP Private Cloud](#)

Introducción

Este documento describe el procedimiento para generar un par de claves SSH usando PuTTY y utilizando un shell de Linux, agréguelo a AMP y luego acceda a la CLI. El dispositivo AMP Private Cloud utiliza autenticación basada en certificados para SSH en el dispositivo. Aquí se detalla el procedimiento para generar rápidamente un par de claves para acceder a la CLI e interactuar con el sistema de archivos a través de SCP (WinSCP).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PuTTY
- WinSCP
- Shell Linux/Mac

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

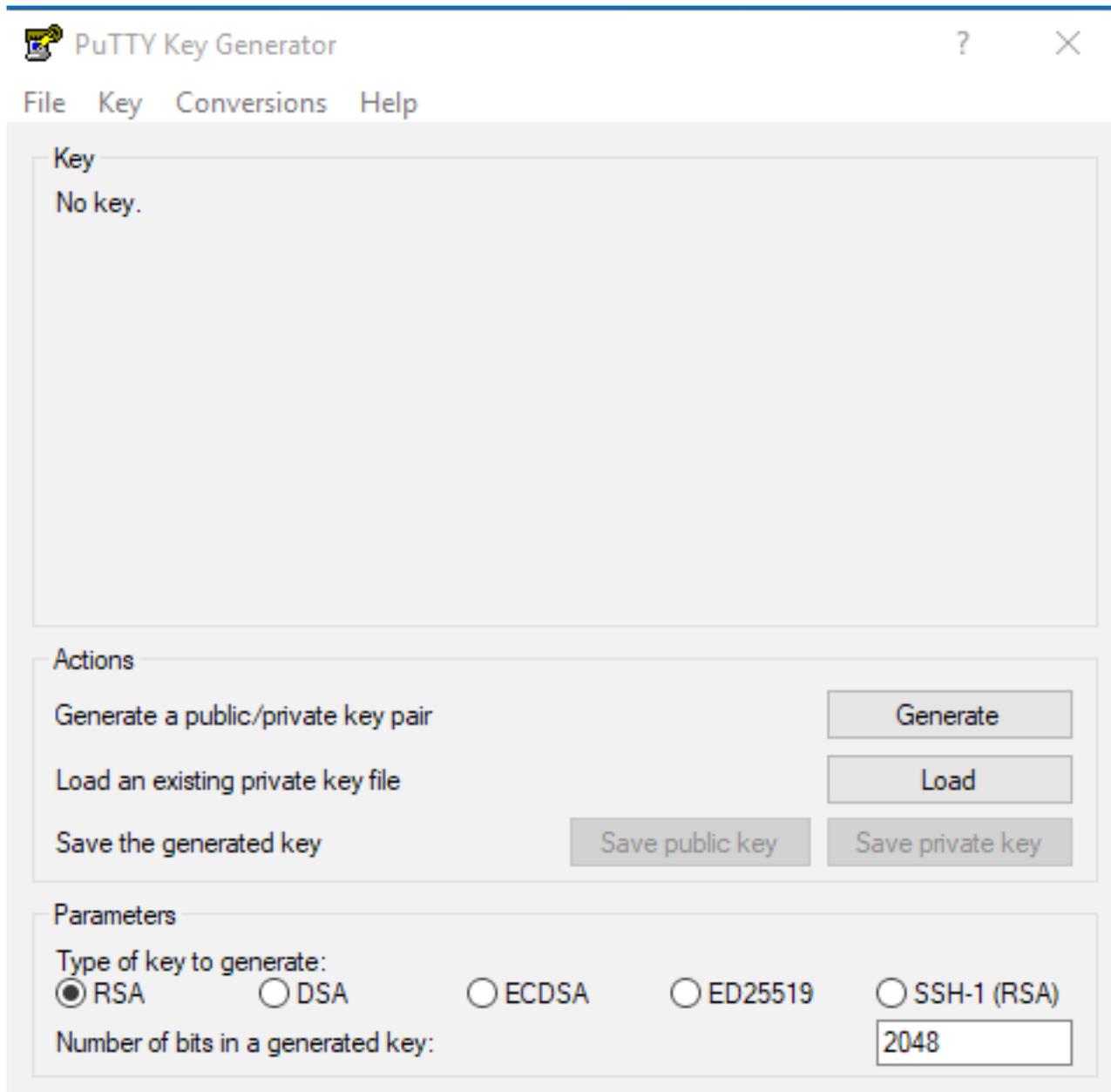
Configurar

El primer paso implica generar un par de claves RSA usando PuTTY o el shell Linux. Después de esto, AMP Private Cloud Appliance debe agregar y confiar en la clave pública.

Generar un par de claves RSA mediante PuTTY

Paso 1. Asegúrese de que ha instalado PuTTY completamente.

Paso 2. Inicie PuTTYGen que se instala junto con PuTTY para generar el par de claves RSA.



Paso 3. Haga clic en Generar para y mueva el cursor aleatoriamente para completar la generación del par de claves.

Paso 4. Elija "Guardar clave pública" y "Guardar clave privada" que se utilizará en las secciones posteriores, como se muestra en la imagen aquí.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajlpb
K3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF
+69l2K7DuVyqhfclH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy
+ShZ8GII0vxxenlin5yY3IUjm8B9xmsPY/norzytm
```

Key fingerprint: ssh-rsa 2047 32:c3:07:60:8f:e4:75:e6:2d:b1:b4:1d:21:18:43:cb

Key comment: rsa-key-20190410

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair

Generate

Load an existing private key file

Load

Save the generated key

Save public key

Save private key

Parameters

Type of key to generate:

 RSA DSA ECDSA ED25519 SSH-1 (RSA)

Number of bits in a generated key:

2048

Paso 5. Abra la clave pública con el Bloc de notas, ya que el formato debe modificarse para que se acepte en el Portal de administración de la nube privada de AMP.



```
----- BEGIN SSH2 PUBLIC KEY -----
```

```
Comment: "rsa-key-20190410"
```

```
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajl
pbK3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF+16
9l2K71DuVyqhfclH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy+ShZ8GII0vx
xenIin5yY3IUjm8B9xmsPY/norzytm+Wh6h0HdQtfgYBAj6TxGbcdK5VcLFaxbMB
CR8cEMx2yW6lUb2DSUwL78eDkFRhf1VWey07HbQ5zm/KPkijNXFCrk9BAmVXvPW4
w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p
```

```
----- END SSH2 PUBLIC KEY -----
```

Paso 6. Elimine las dos primeras líneas que comienzan por "—BEGIN" y la última que comienza por "— END"

Paso 7. Elimine todos los saltos de línea para hacer que el contenido de la clave pública sea una sola línea continua.

Paso 8. Introduzca la palabra "ssh-rsa" al principio del archivo. Guarde el archivo.

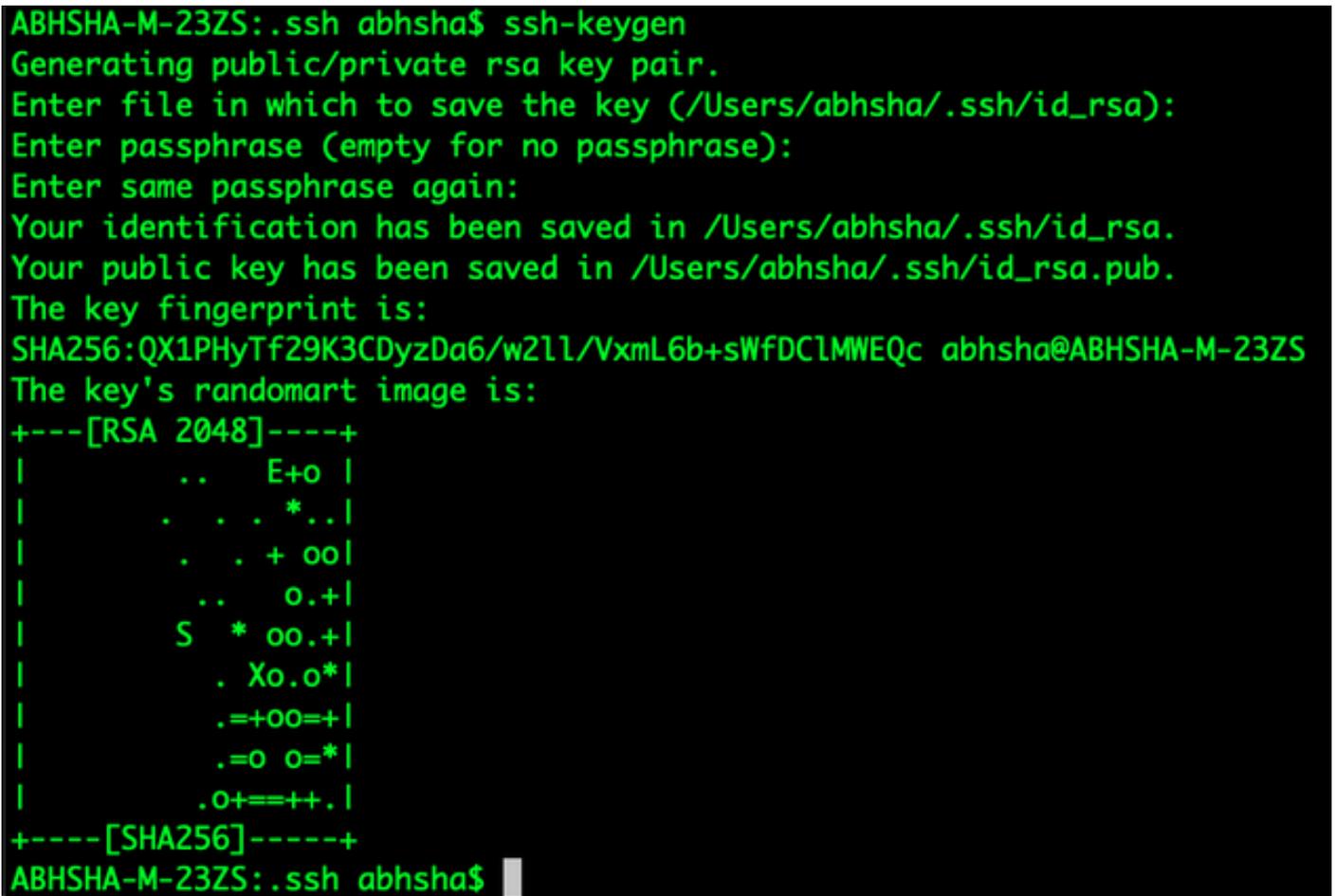


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAQBAn/DObg8zkYwHaMfq011V1GcLL7c fgvj8aj1pbK3+2mXon1nr4YP8S+oDsxdl/b6QV899kC7z3sQevpXxC9sC1Guh+nv8WAunF+16912K71DuVyqhfcLH/vv5hPHJKaC47BqdWs
+AudrcUqoDw0rHREHy+ShZ8GII0vxxenIIn5yY3IUjm889xmsPY/norztyt
m+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbHBCR8cEHx2yw61Ub2DSUwL78eDkFRhf1VWey07HbQ5zm/KPk1jIXFCrk9BAmXvPW4w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p
```

Genere un par de llaves RSA usando Linux/Mac

Paso 1. En la CLI de Linux/Mac, ingrese el comando "ssh-keygen"

Paso 2. Introduzca los parámetros necesarios y esto genera el par de claves RSA en la carpeta "~/.ssh"



```
ABHSHA-M-23ZS:~.ssh abhsha$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/abhsha/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/abhsha/.ssh/id_rsa.
Your public key has been saved in /Users/abhsha/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:QX1PhyTf29K3CDyzDa6/w21l/VxmL6b+sWfDClMWEQc abhsha@ABHSHA-M-23ZS
The key's randomart image is:
+----[RSA 2048]-----+
|          ..  E+o |
|          . . . *..|
|          . . + oo|
|          ..  o.+|
|          S * oo.+|
|          . Xo.o*|
|          .+=+oo=+|
|          .=o o=*|
|          .o+==++.|
+-----[SHA256]-----+
ABHSHA-M-23ZS:~.ssh abhsha$
```

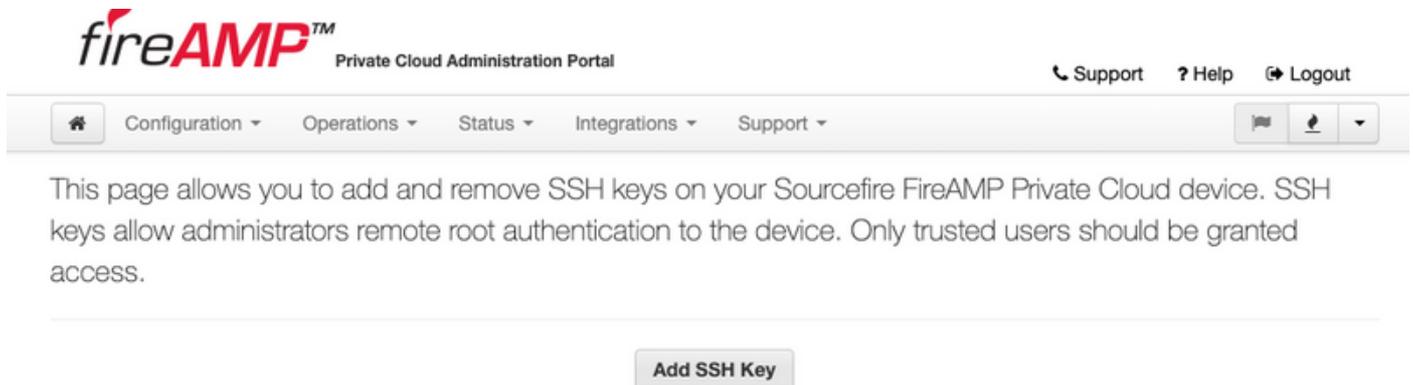
Paso 3. Si abre el contenido de id_rsa.pub, que es la clave pública, puede ver que ya está en el formato requerido.

```
ABHSHA-M-23ZS:~# ssh abhsha$
ABHSHA-M-23ZS:~# ssh abhsha$ ls
id_rsa          id_rsa.pub      known_hosts
ABHSHA-M-23ZS:~# ssh abhsha$
ABHSHA-M-23ZS:~# ssh abhsha$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ
5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeFU11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+y
VMT2wrHGEyxNyWZ0ZL04Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbXk1ByTVcqGYL3P4JCfMth4tCQDyPd/
CWAIA/263oVDwS4eWEL7haZS+zsQGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2
JUL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
ABHSHA-M-23ZS:~# ssh abhsha$
```

Adición de las claves públicas generadas al portal de administración de AMP para nube privada

Paso 1. Vaya a AMP Private Cloud Administration Portal > Configuration > SSH

Paso 2. Haga clic en "Agregar clave SSH".



Paso 3. Agregue el contenido de la clave pública y guárdelo.

SSH Key

Name

Enabled

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeF
U11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+yVMT2wrHGEyxNyWZ0ZL04Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbX
k1ByTVcqGYL3P4JCfMth4tCQDyPd/CWAIA/263oVDwS4eWEL7haZS+zsQGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2
JUL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
```

✓ Save × Cancel

Paso 4. Una vez guardado, asegúrese de que está "reconfigurando" el dispositivo.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Configuration Changed

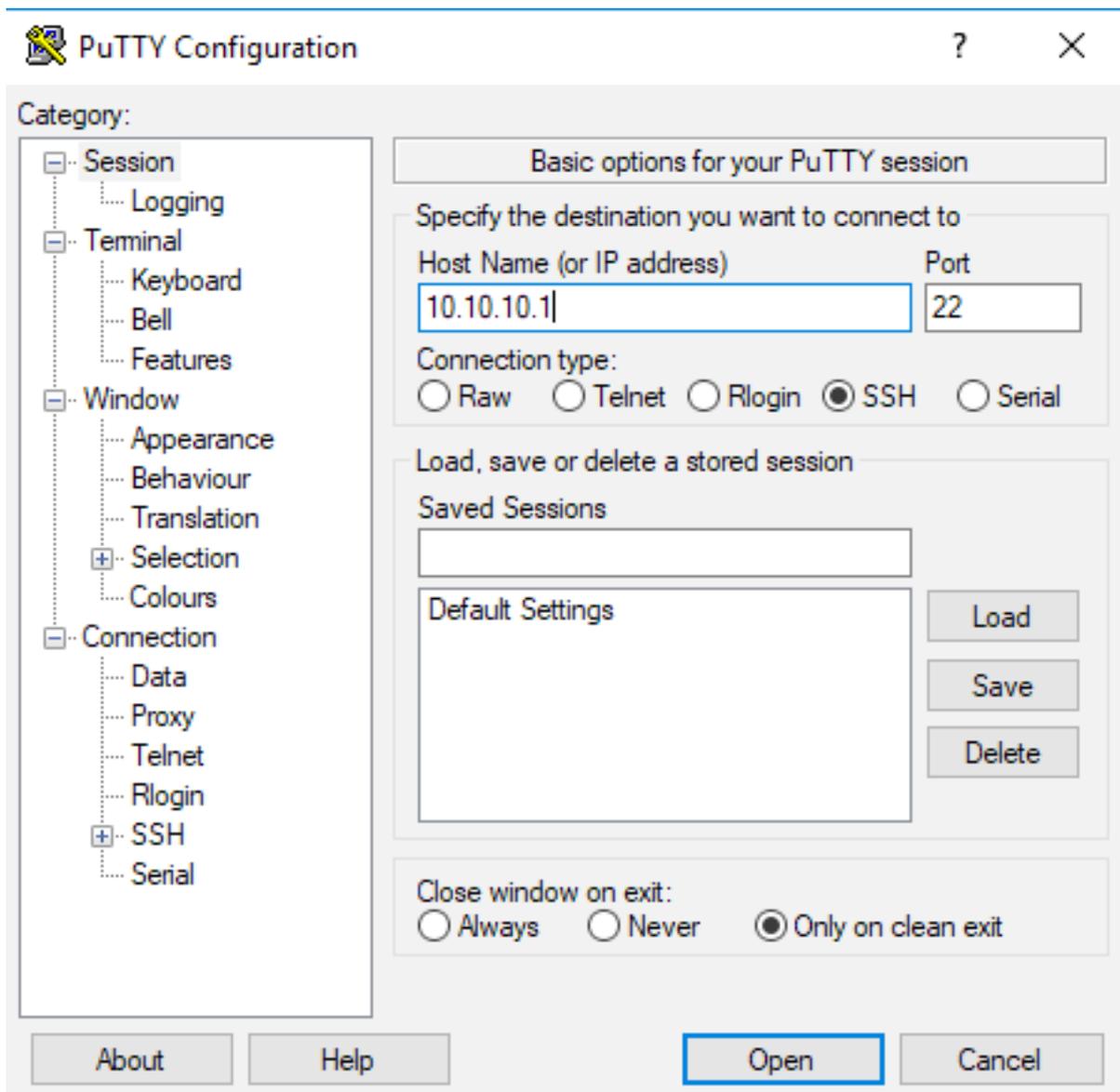
Configuration changes do not take effect until reconfiguration is performed.

 **Reconfigure Now**

Reconfiguration

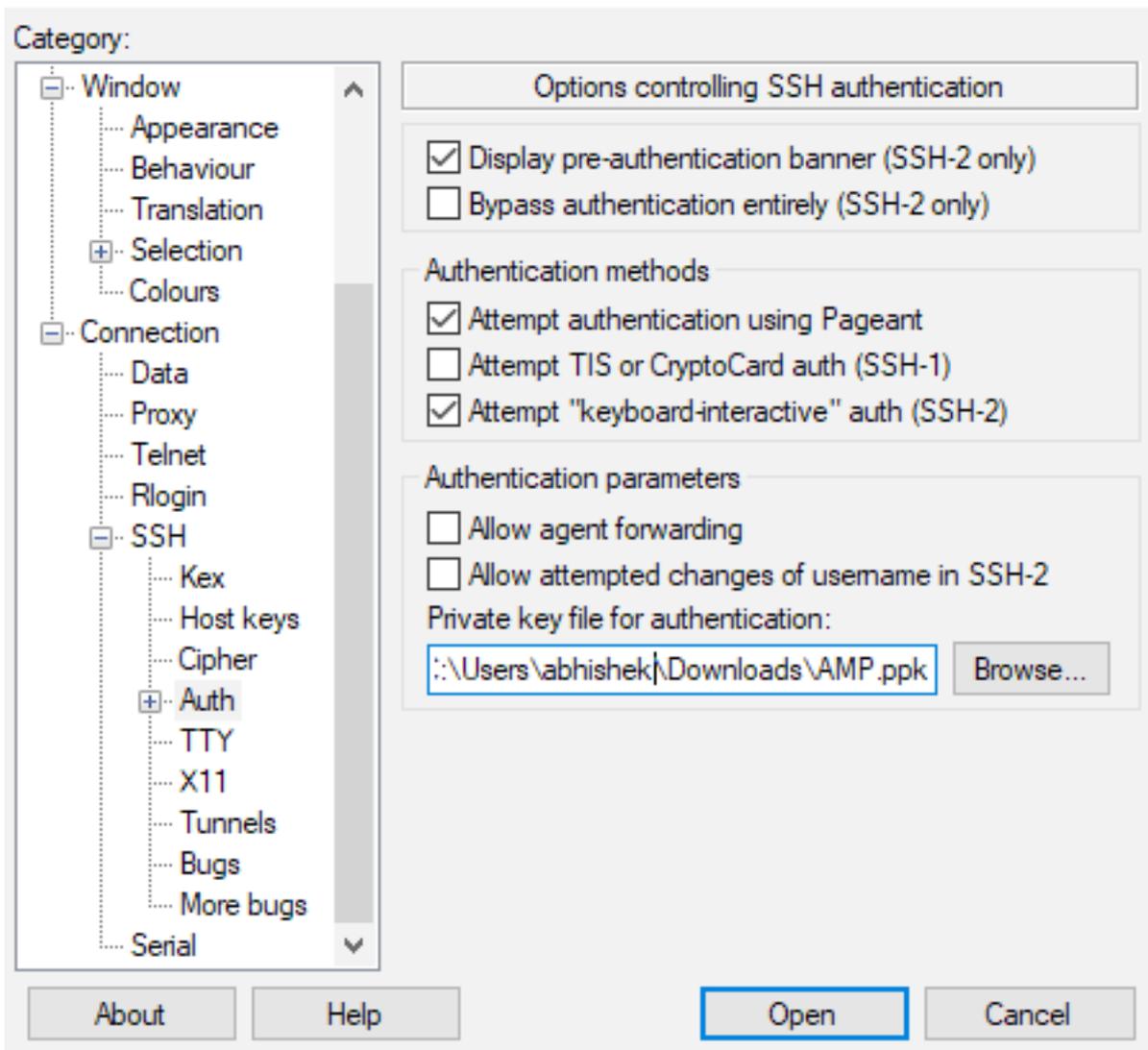
Utilice el par de claves generado para SSH en el dispositivo mediante PuTTY

Paso 1. Abra PuTTY e introduzca la dirección IP del portal de administración de nube privada de AMP.



Paso 2. En el panel izquierdo, seleccione Connection > SSH y haga clic en Auth.

Paso 3. Seleccione la clave privada generada por PuTTYGen. Este es un archivo PPK.



Paso 4. Haga clic en Open (Abrir) y, cuando solicite un nombre de usuario, introduzca "root" (raíz) y debería acceder a la CLI de AMP Private Cloud.

Uso del par de claves configurado para SSH en el dispositivo mediante Linux

Paso 1. Si los pares de claves privada y pública se almacenan correctamente en la ruta `~/.ssh`, debería poder enviar SSH al dispositivo AMP Private Cloud simplemente ejecutando el comando `ssh` sin pedirle ninguna contraseña.

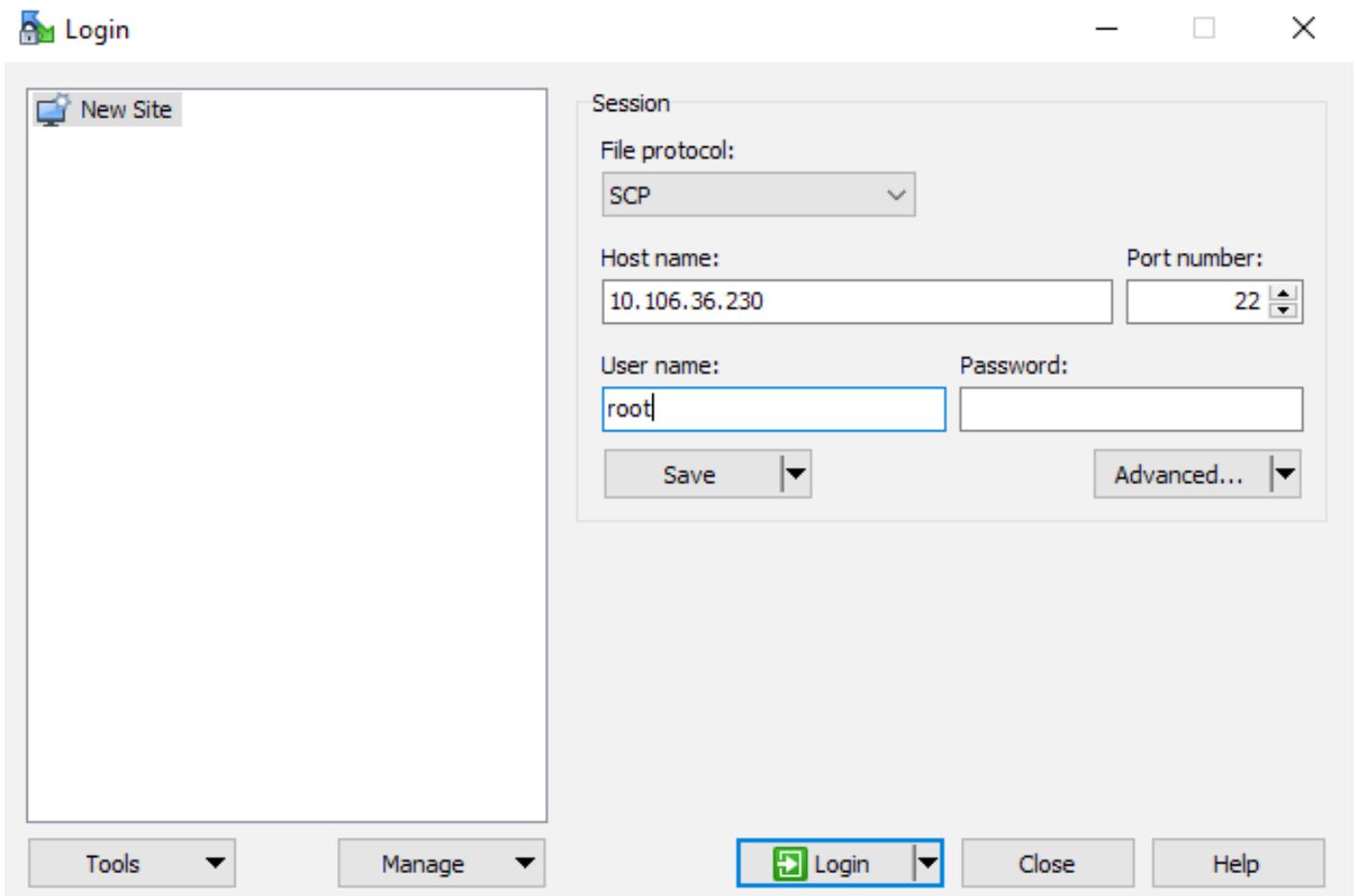
```
ssh root@<AMP-IP-ADDRESS>
```

```
[abhishek@supecomputer .ssh]$ ssh root@10.106.36.230
The authenticity of host '10.106.36.230 (10.106.36.230)' can't be established.
RSA key fingerprint is SHA256:mvHHLqnMJhPBBBpPankbdXV7pJxBha5NE1h1GdBs1fg.
RSA key fingerprint is MD5:27:78:7c:39:de:b9:b7:d8:45:87:8e:09:96:33:b6:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.106.36.230' (RSA) to the list of known hosts.
Last login: Fri Mar 29 03:30:46 2019 from 173.39.68.177
[root@fireamp ~]#
[root@fireamp ~]#
```

Uso de WinSCP para interactuar con el sistema de archivos de AMP Private Cloud

Paso 1. Instale WinSCP en su equipo e inícielo.

Paso 2. Introduzca la dirección IP del Portal de administración de la nube privada de AMP y seleccione el Protocolo de archivo como SCP. Introduzca el nombre de usuario como raíz y deje el campo de contraseña.



Paso 3. Seleccione Advanced > Advanced > SSH > Authentication

Paso 4. Seleccione el archivo PPK que PuTTYgen generó como clave privada.

Advanced Site Settings



Environment

- Directories
- Recycle bin
- Encryption
- SFTP
- SCP/Shell

Connection

- Proxy
- Tunnel

SSH

- Key exchange
- Authentication**
- Bugs

Note

Bypass authentication entirely

Authentication options

- Attempt authentication using Pageant
- Attempt 'keyboard-interactive' authentication
 - Respond with password to the first prompt
- Attempt TIS or CryptoCard authentication (SSH-1)

Authentication parameters

- Allow agent forwarding

Private key file:

Display Public Key Tools ▾

GSSAPI

- Attempt GSSAPI authentication
 - Allow GSSAPI credential delegation

Color ▾ OK Cancel Help

Paso 5. Haga clic en Aceptar y, a continuación, en Iniciar sesión. Debe poder iniciar sesión correctamente después de aceptar el mensaje.