

Acesso ao CLI da nuvem privada da AMP via SSH e transferência de arquivos via SCP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Gerar um par de chaves RSA usando PuTTY](#)

[Gerar um par de chaves RSA usando Linux/Mac](#)

[Adição das chaves públicas geradas ao portal AMP Private Cloud Administration](#)

[Usar o par de chaves gerado para SSH no dispositivo usando PuTTY](#)

[Usando o par de chaves configurado para SSH no dispositivo usando Linux](#)

[Usando o WinSCP para interagir com o sistema de arquivos da AMP Private Cloud](#)

Introduction

Este documento descreve o procedimento para gerar um par de chaves SSH usando PuTTY e usando um shell Linux, adicioná-lo ao AMP e, em seguida, acessar o CLI. O dispositivo AMP Private Cloud usa autenticação baseada em certificado para SSH no dispositivo. O procedimento para gerar um par de chaves rapidamente, a fim de acessar a CLI e interagir com o sistema de arquivos via SCP (WinSCP) é detalhado aqui.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PuTTY
- WinSCP
- shell Linux / Mac

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

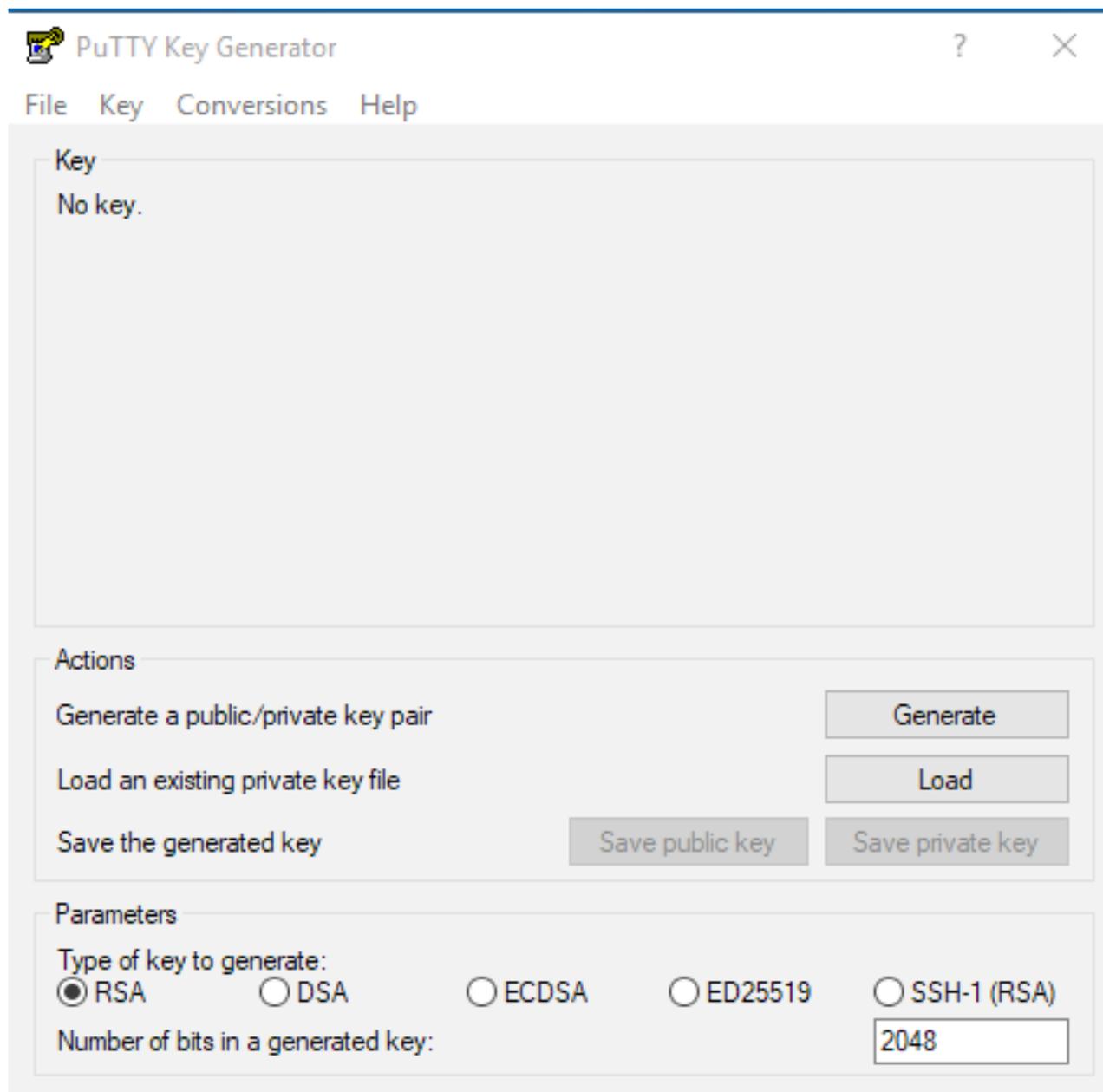
Configurar

A primeira etapa envolve a geração de um par de chaves RSA usando PuTTY ou shell Linux. Depois disso, a chave pública precisa ser adicionada e confiável pelo AMP Private Cloud Appliance.

Gerar um par de chaves RSA usando PuTTY

Etapa 1. Verifique se você instalou o PuTTY completamente.

Etapa 2. Inicie o PuTTYGen instalado junto com o PuTTY para gerar o par de chaves RSA.



Etapa 3. Clique em Gerar para e mova o cursor aleatoriamente para concluir a geração do par de chaves.

Etapa 4. Escolha "Save public key" (Salvar chave pública) e "Save private key" (Salvar chave privada), que serão usadas nas seções posteriores, como mostrado na imagem aqui.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajlpb
K3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF
+69l2K7lDuVyqhfclH/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

Etapa 5. Abra a chave pública com o Notepad, pois o formato precisa ser modificado para que seja aceito no AMP Private Cloud Administration Portal.



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

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

```
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajl
pbK3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF+16
9l2K7lDuVyqhfclH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy+ShZ8GII0vx
xenIin5yY3IUjm8B9xmsPY/norzytm+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbMB
CR8cEMx2yW6lUb2DSUwL78eDkFRhf1VWey07HbQ5zm/KPkijNXFCrk9BAmVXvPW4
w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p
```

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

Etapa 6. Remova as duas primeiras linhas que começam com "—BEGIN" e a última linha que começa com "—END"

Passo 7. Remova todas as quebras de linha para tornar o conteúdo da chave pública como uma única linha contínua.

Etapa 8. Digite a palavra "ssh-rsa" no início do arquivo. Salve o arquivo.

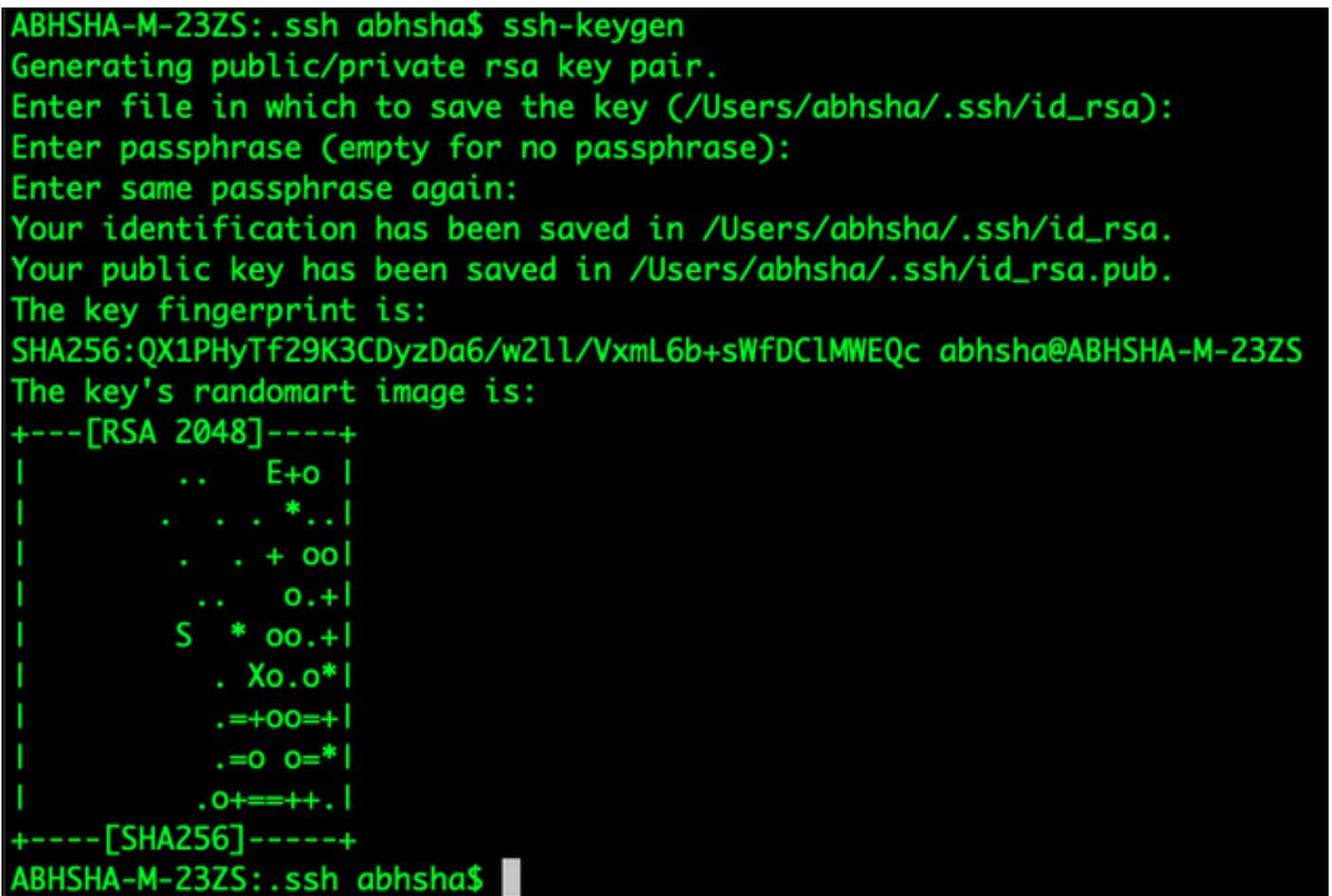


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAQBAn/DObg8zkYWhaMfq0i1V1GcLL7cFgvj8aj1pbK3+2mXon1nr4YP85+oDsxdI/b6QV899kc7z3sQevpXxC9sC1Guh+nv8NAunF+16912K71DuVyqhfcLH/vv5MPhJKaC47BqdWs
+AudrcUqoDw0rHREHy+ShZ8GII0vxxenIIn5yY3Iujm889xmsPY/norzyt
m+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxhMBCRBcEHx2yw61Ub2DSUwL78eDkFRhf1VWey07HbQ5zm/KPk1jIXFCrk98AmXvPW4w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p
```

Gerar um par de chaves RSA usando Linux/Mac

Etapa 1. Na CLI do Linux/Mac, digite o comando "ssh-keygen"

Etapa 2. Insira os parâmetros necessários e isso gera o par de chaves RSA na pasta "~/ssh"



```
ABHSHA-M-23ZS:~$ 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/w2l1/VxmL6b+sWfDC1MWEQc 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:~$
```

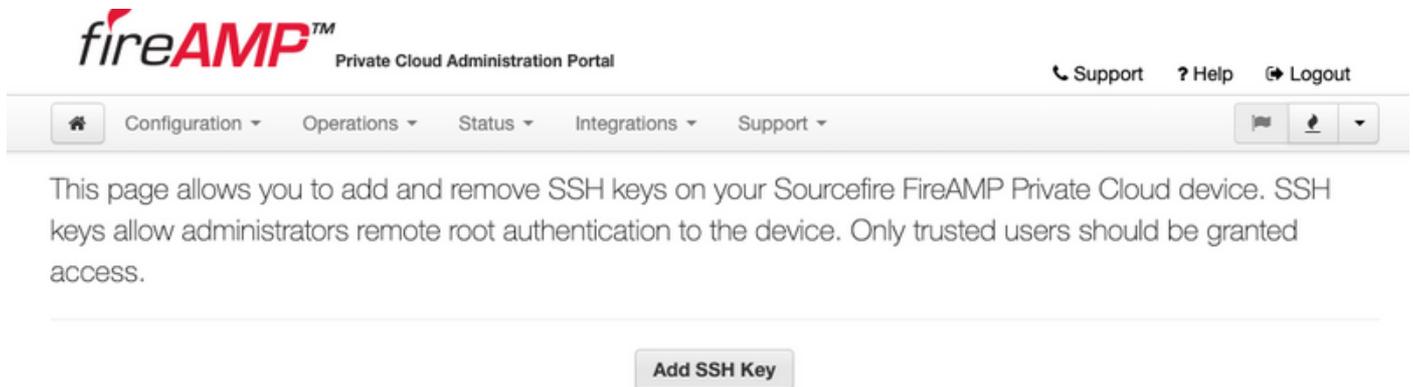
Etapa 3. Se você abrir o conteúdo de id_rsa.pub, que é a chave pública, poderá ver que ele já está no formato necessário.

```
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/K2J
JL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
ABHSHA-M-23ZS: .ssh abhsha$
```

Adição das chaves públicas geradas ao portal AMP Private Cloud Administration

Etapa 1. Navegue até AMP Private Cloud Administration Portal > Configuration > SSH

Etapa 2. Clique em "Add SSH Key" (Adicionar chave SSH)



Etapa 3. Adicione o conteúdo da chave pública e salve-o.

SSH Key

Name

AMP-TEST|

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

Etapa 4. Depois que isso for salvo, verifique se você está "Reconfigurando" o dispositivo.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Configuration Changed

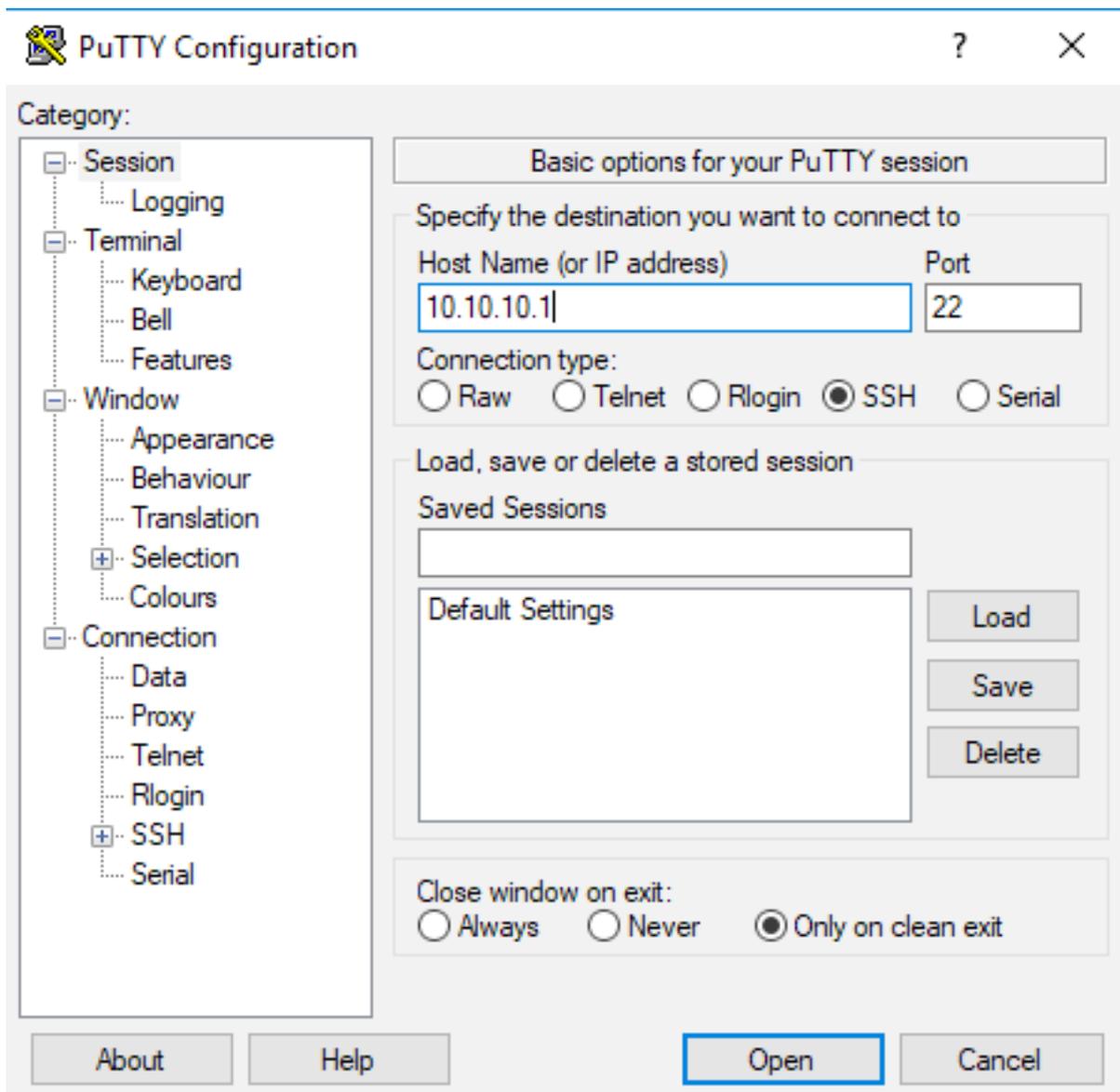
Configuration changes do not take effect until reconfiguration is performed.

 **Reconfigure Now**

Reconfiguration

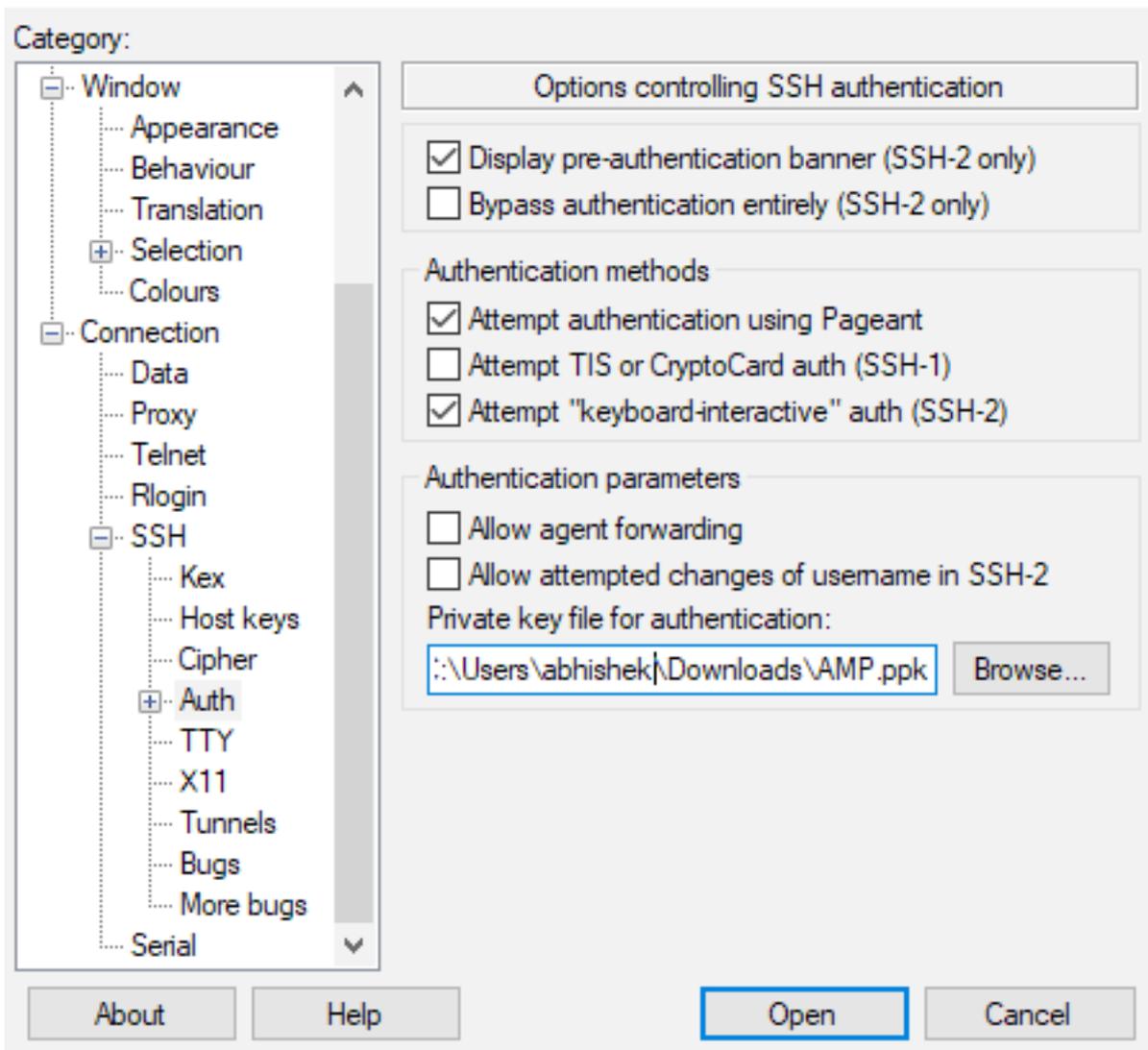
Usar o par de chaves gerado para SSH no dispositivo usando PuTTY

Etapa 1. Abra o PuTTY e insira o endereço IP do portal AMP Private Cloud Administration.



Etapa 2. No painel esquerdo, selecione Connection > SSH e clique em Auth.

Etapa 3. Selecione a chave privada gerada por PuTTYGen. Este é um arquivo PPK.



Etapa 4. Clique em Open (Abrir) e, quando solicitar um nome de usuário, digite "root" (raiz) e você deve pousar na CLI da nuvem privada da AMP.

Usando o par de chaves configurado para SSH no dispositivo usando Linux

Etapa 1. Se os pares de chave privada e pública estiverem armazenados corretamente no caminho `~/.ssh`, você deverá conseguir SSH para o dispositivo AMP Private Cloud simplesmente emitindo o comando `ssh` sem solicitar qualquer senha.

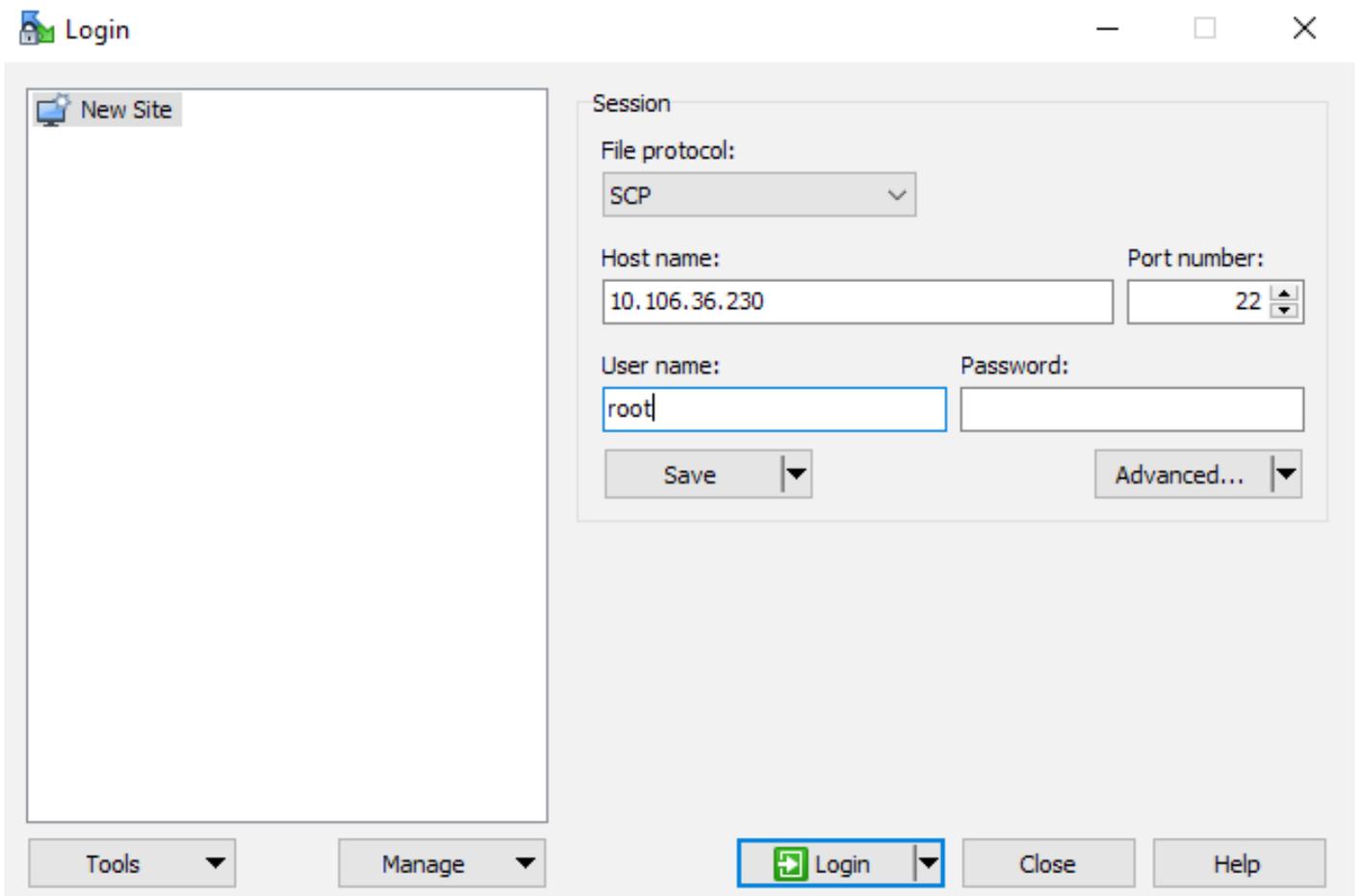
```
ssh root@<AMP-IP-ADDRESS>
```

```
[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 ~]#
```

Usando o WinSCP para interagir com o sistema de arquivos da AMP Private Cloud

Etapa 1. Instale o WinSCP na sua máquina e inicie-o.

Etapa 2. Insira o endereço IP do AMP Private Cloud Administration Portal e selecione File Protocol como SCP. Digite o nome de usuário como raiz e deixe o campo senha.



Etapa 3. Selecione Avançado > Avançado > SSH > Autenticação

Etapa 4. Selecione o arquivo PPK que foi gerado como chave privada pelo PuTTYgen.

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

Etapa 5. Clique em OK e em Login. Você deve conseguir fazer login com êxito após aceitar o prompt.