

# SSHによるAMPプライベートクラウドのCLIへのアクセスおよびSCPによるファイルの転送

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[PuTTYを使用したRSAキーペアの生成](#)

[Linux/Macを使用したRSAキーペアの生成](#)

[生成された公開キーをAMPプライベートクラウド管理ポータルに追加する](#)

[生成されたキーペアを使用して、PuTTYを使用してアプライアンスにSSH接続します](#)

[設定されたキーペアを使用して、Linuxを使用してアプライアンスにSSH接続する](#)

[WinSCPを使用したAMPプライベートクラウドのファイルシステムとの対話](#)

## 概要

このドキュメントでは、PuTTYとLinuxシェルを使用してSSHキーペアを生成し、それをAMPに追加してからCLIにアクセスする手順について説明します。AMPプライベートクラウドアプライアンスは、証明書ベースの認証を使用してアプライアンスにSSH接続します。CLIにアクセスし、SCP(WinSCP)を介してファイルシステムとやり取りするために、キーペアを迅速に生成する手順について詳しく説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- PuTTY
- WinSCP
- Linux/Macシェル

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

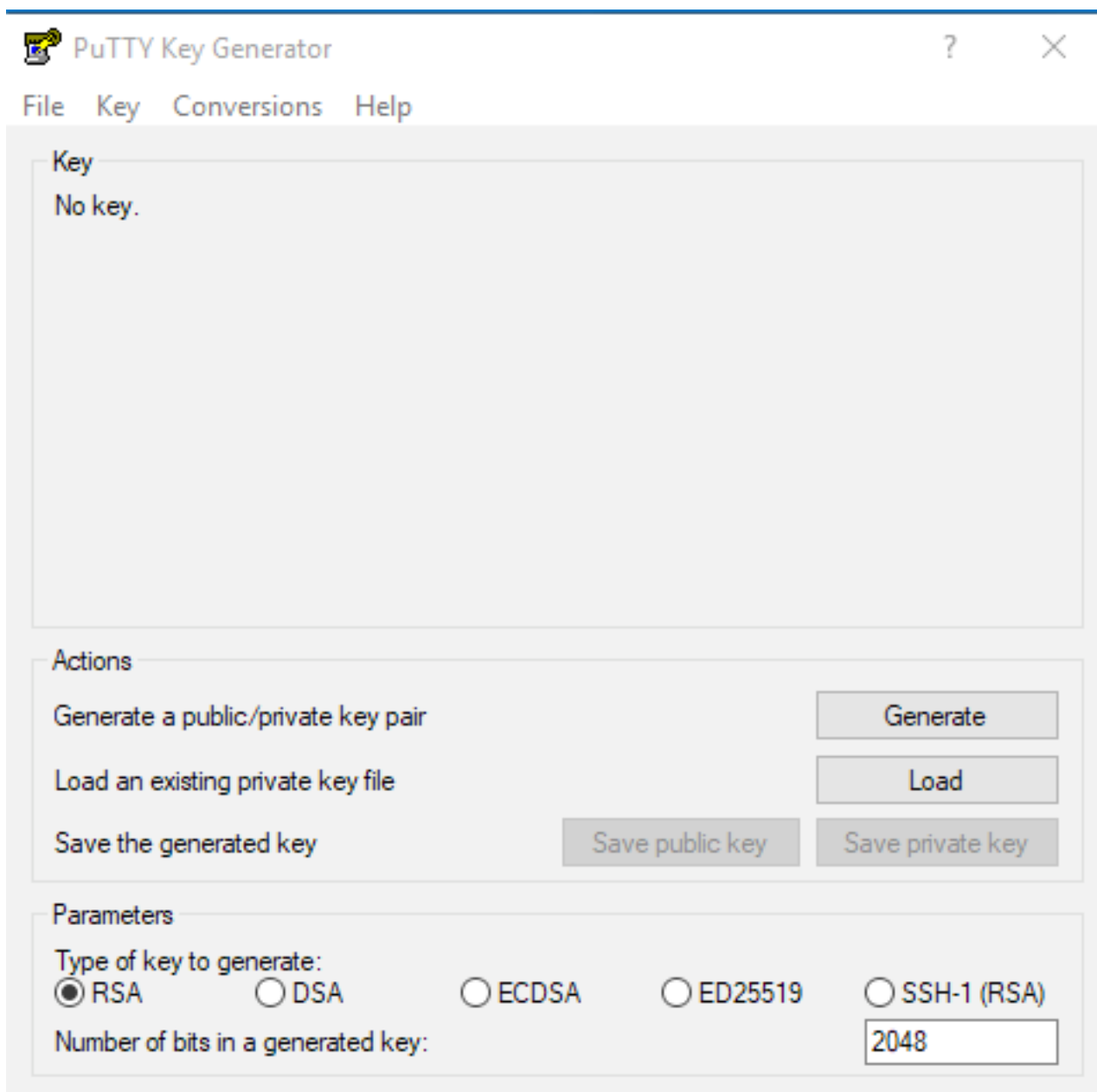
# 設定

最初のステップでは、PuTTYまたはLinuxシェルを使用してRSAキーペアを生成します。その後、AMPプライベートクラウドアプライアンスによって公開キーを追加し、信頼する必要があります。

## PuTTYを使用したRSAキーペアの生成

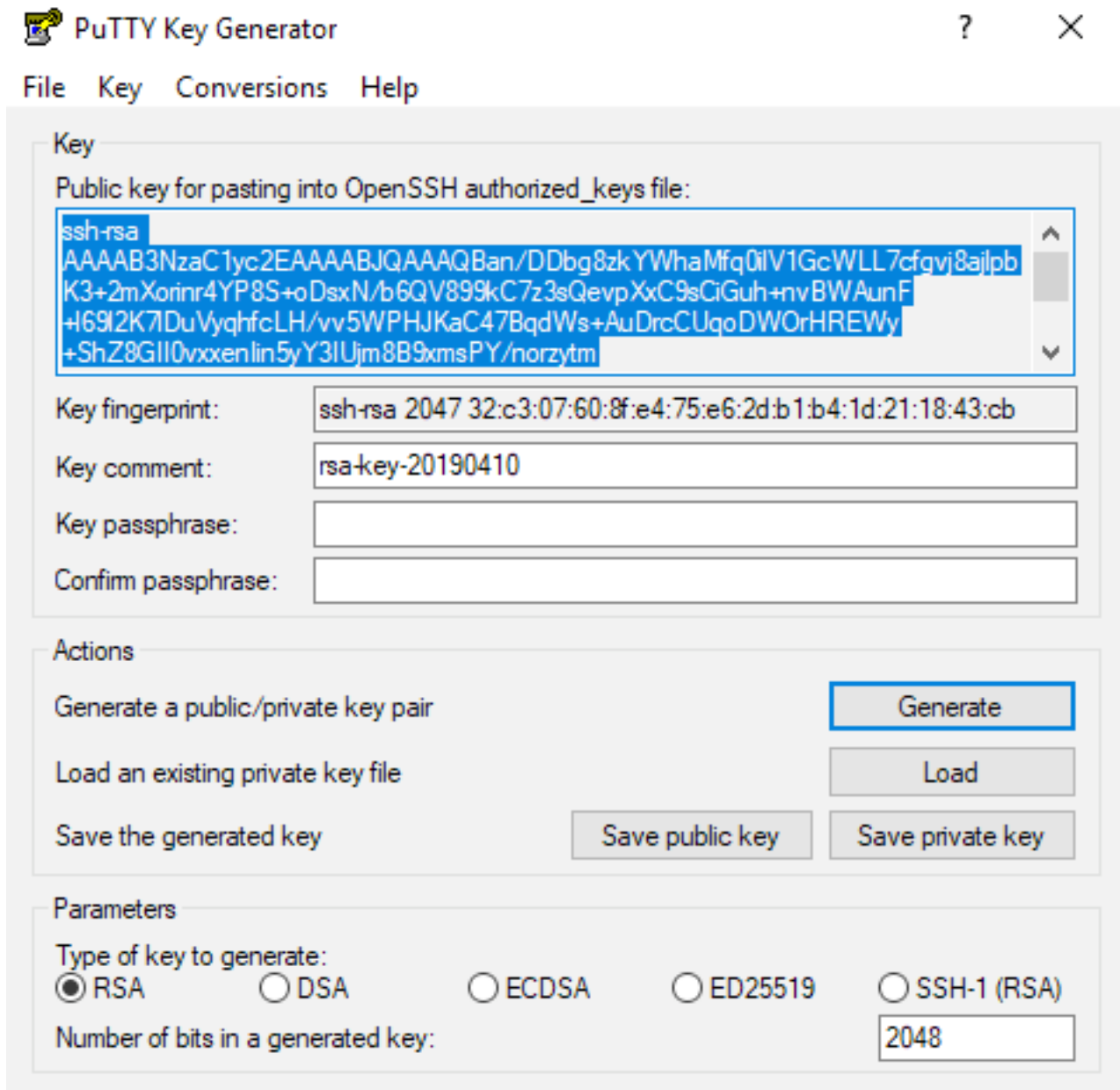
ステップ1:PuTTYが完全にインストールされていることを確認します。

ステップ2:PuTTYとともにインストールされるPuTTYGenを起動して、RSAキーペアを生成します。



ステップ3:[Generate]をクリックしてカーソルをランダムに移動し、キーペアの生成を完了します。

ステップ4: 次の図に示すように、後のセクションで使用する[Save public key]と[Save private key]を選択します。



ステップ5:AMPプライベートクラウド管理ポータルで承認するには、形式を変更する必要があるため、メモ帳で公開キーを開きます。

AMP-VPC - Notepad


File Edit Format View Help

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: "rsa-key-20190410"  
AAAAB3NzaC1yc2EAAAABJQAAAQBan/DDbg8zkYWhaMfq0ilV1GcWLL7cfgvj8ajl  
pbK3+2mXorinr4YP8S+oDsxN/b6QV899kC7z3sQevpXxC9sCiGuh+nvBWAunF+16  
9l2K71DuVyqhfclH/vv5WPHJKaC47BqdWs+AuDrcCUqoDWOrHREWy+ShZ8GII0vx  
xenIin5yY3IUjm8B9xmsPY/norzytm+Wh6h0HdQtfgyBAj6TxGbcdK5VcLFaxbMB  
CR8cEMx2yW61Ub2DSUwL78eDkfrhf1Vwey07HbQ5zm/KPkiJNXFCrk9BAmVXvPW4  
w5FZSKKYQJgns1pjggcmpPbR879ib1xz7neUG+ktj16T4G3p  
----- END SSH2 PUBLIC KEY -----
```

ステップ6: 「- BEGIN」で始まる最初の2行と「- END」で始まる最後の行を削除します

ステップ7: すべての改行を削除して、公開キーのコンテンツを1行の連続として作成します。

ステップ8: ファイルの先頭に「ssh-rsa」と入力します。ファイルを保存します。

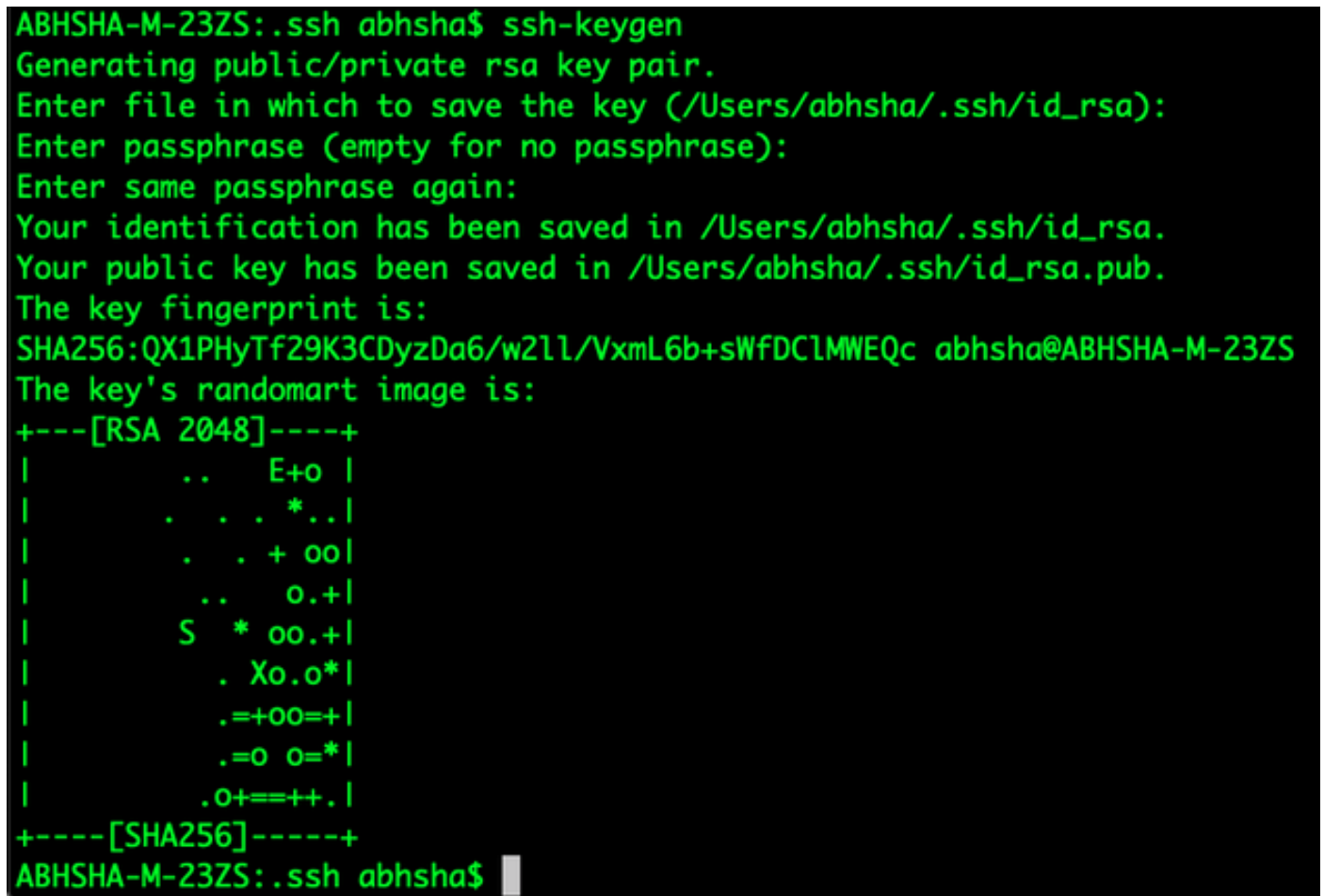


```
AMP-VPC - Notepad
File Edit Format View Help
ssh-rsa AAAAB3NzaC1yc2EAAAQBan/DDbg8zkYhhaMfq011V1GcLL7cFgvj8aj1pbK3+2mXorinr4YP8S+oDsxl/b6QV899kC7z3sQevpXxC9sC1Guh+nv8WAunF+16912K71DuVyqhfcLH/vv5WPHJKaC47BqdWs
+AuDrcCUqoDw0rHREWy+ShZ8GII0vxxenIin5yY3IUjm889xmsPY/norzyt
m+Wh6h8HdQtfgYBAj6TxGbcdK5VcLFaxbBRCR8cEMxZyW6IUb2DSUwL78e0kfRhf1VWey07HbQ5zm/KPk1jNXCrcrk98AmVXvPW4w5FZSKKYQJgns1pjggcmpPbR8791b1xz7neUG+ktj16T4G3p
```

## Linux/Macを使用したRSAキーペアの生成

ステップ1: Linux/Mac CLIで、コマンド「ssh-keygen」を入力します

ステップ2: 必要なパラメータを入力すると、「~/.ssh」フォルダにRSAキーペアが生成されます



```
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$
```

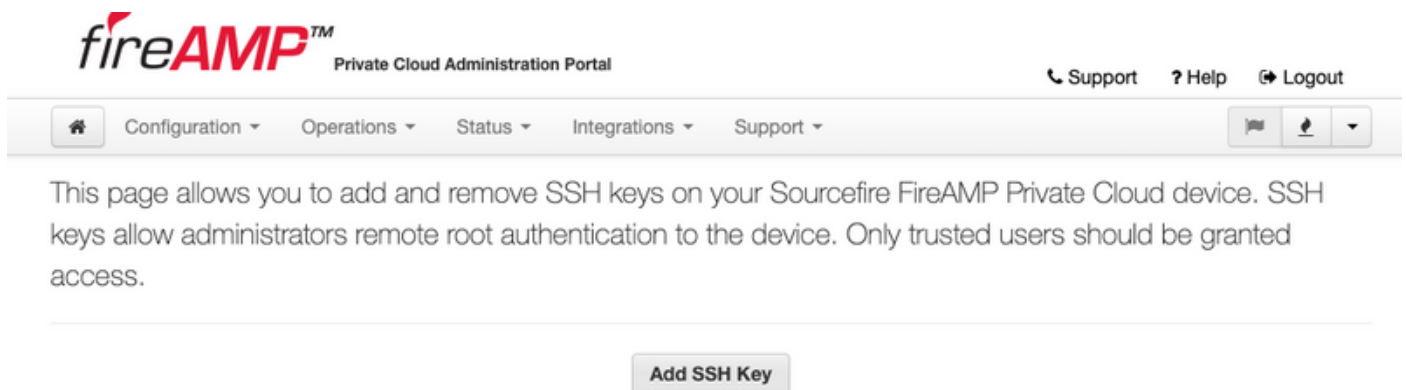
ステップ3: 公開キーであるid\_rsa.pubの内容を開くと、すでに必要な形式になっていることがわかります。

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

## 生成された公開キーをAMPプライベートクラウド管理ポータルに追加する

ステップ1:[AMP Private Cloud Administration Portal] > [Configuration] > [SSH]に移動します

ステップ2:[Add SSH Key]をクリックします



ステップ3：公開キーの内容を追加して保存します。

### 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

ステップ4：これが保存されたら、アプライアンスを「再設定」していることを確認します。



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

### ⚙ Configuration Changed

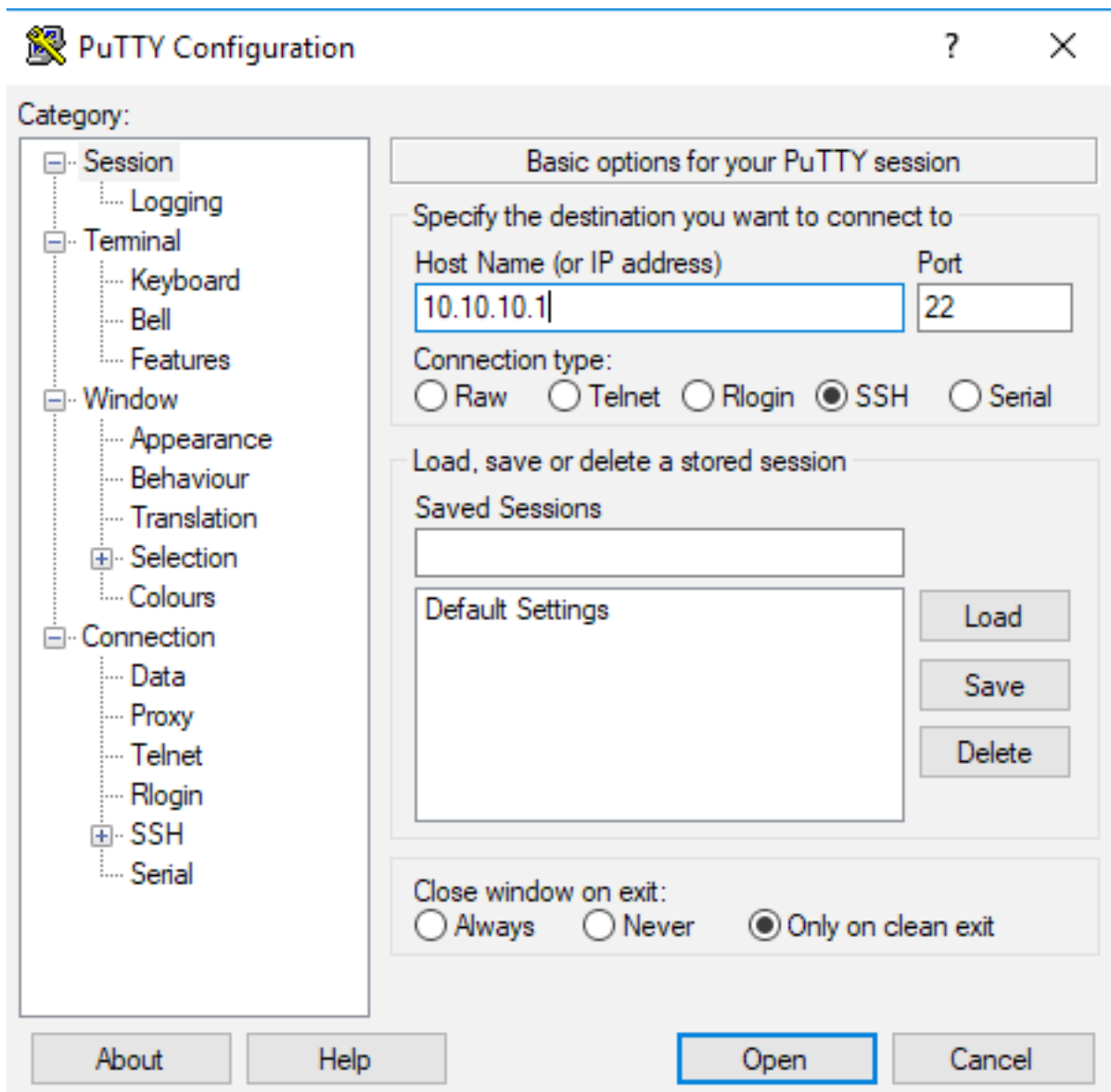
Configuration changes do not take effect until reconfiguration is performed.

⚙ Reconfigure Now

Reconfiguration

生成されたキーペアを使用して、PuTTYを使用してアプライアンスにSSH接続します

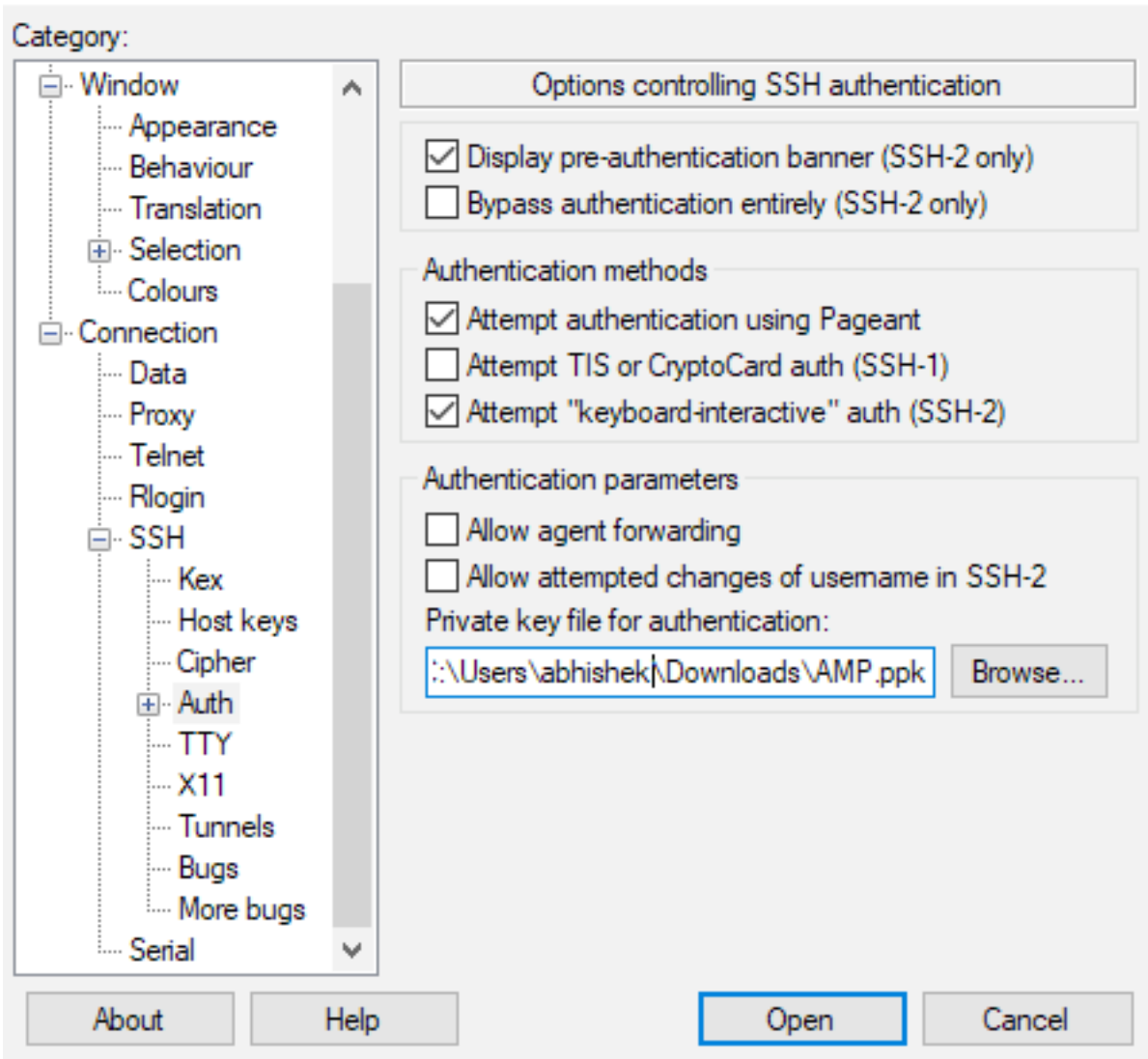
ステップ1:PuTTYを開き、AMPプライベートクラウド管理ポータル(IPアドレス)を入力します。



ステップ2：左側のペインで[Connection] > [SSH]を選択し、[Auth]をクリックします。

ステップ3:PuTTYGenによって生成された秘密キーを選択します。これはPPKファイルです。





ステップ4:[Open (開く)]をクリックし、ユーザ名を入力を求められたら、「root」と入力して、AMPプライベートクラウドのCLIに移動します。

## 設定されたキーペアを使用して、Linuxを使用してアプライアンスにSSH接続する

ステップ1：秘密キーと公開キーのペアが `~/.ssh` パスに正しく保存されている場合は、パスワードの入力を求めずに `ssh` コマンドを発行するだけで、AMPプライベートクラウドアプライアンスにSSH接続できます。

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

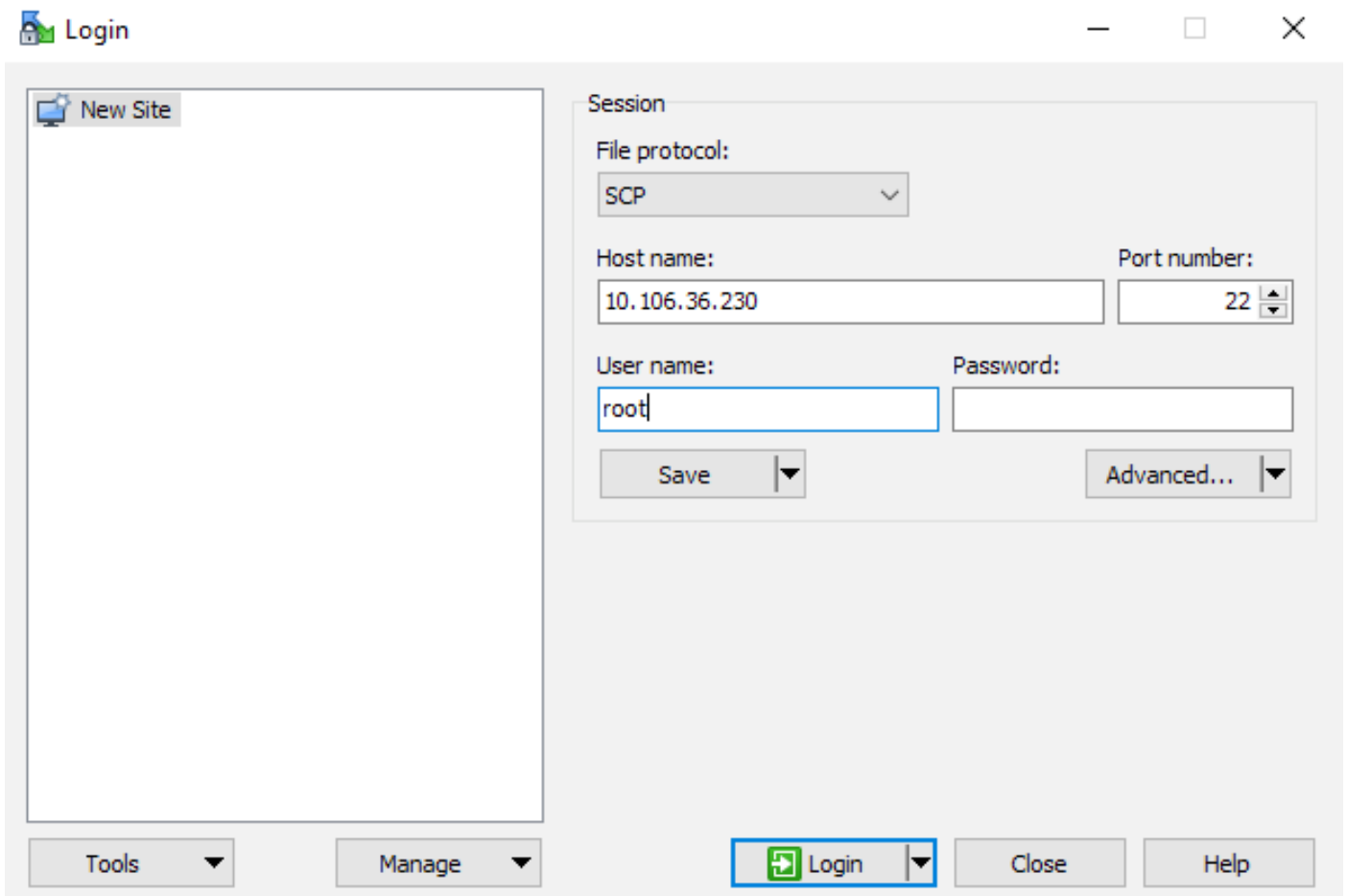


```
[abhishek@supecomputer .ssh]$ ssh root@10.106.36.230
The authenticity of host '10.106.36.230 (10.106.36.230)' can't be established.
RSA key fingerprint is SHA256:mvHHLqnMJhPBBBpPankbdXV7pjxBha5NE1h1GdBs1fg.
RSA key fingerprint is MD5:27:78:7c:39:de:b9:b7:d8:45:87:8e:09:96:33:b6:db.
Are you sure you 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 ~]#
```

## WinSCPを使用したAMPプライベートクラウドのファイルシステムとの対話

ステップ1: マシンにWinSCPをインストールし、起動します。

ステップ2: AMPプライベートクラウド管理ポータルのIPアドレスを入力し、[File Protocol]で[SCP]を選択します。ユーザー名をrootとして入力し、パスワードフィールドを残します。



ステップ3: [Advanced] > [Advanced] > [SSH] > [Authentication]を選択します。

ステップ4: PuTTYgenによって秘密キーとして生成されたPPKファイルを選択します。

## 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

ステップ5:[OK]をクリックし、[Login]をクリックします。プロンプトを受け入れた後、正常にログインできるはずですが。