Zugriff auf die CLI der AMP Private Cloud über SSH und Übertragung von Dateien über SCP

Inhalt

Einführung

In diesem Dokument wird die Vorgehensweise zum Generieren eines SSH-Schlüsselpaars mit PuTTY und unter Verwendung einer Linux-Shell beschrieben. Fügen Sie es zu AMP hinzu, und greifen Sie dann auf die CLI zu. Die AMP Private Cloud-Appliance verwendet eine zertifikatsbasierte Authentifizierung für SSH in der Appliance. Das Verfahren zum schnellen Generieren eines Schlüsselpaars, um auf die CLI zuzugreifen und über SCP (WinSCP) mit dem Dateisystem zu interagieren, wird hier beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- PuTTY
- WinSCP
- Linux/Mac-Shell

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

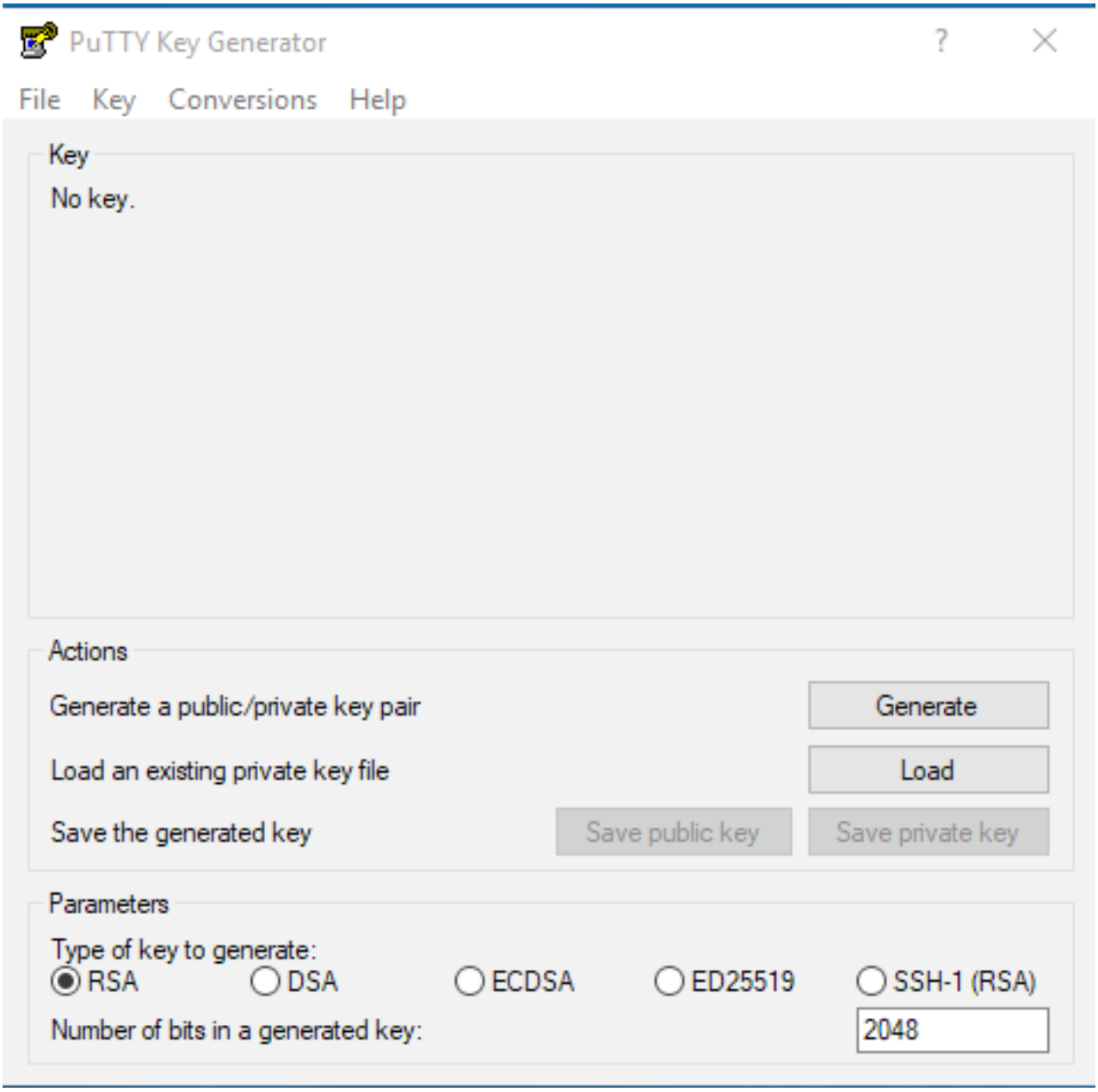
Konfigurieren

Der erste Schritt besteht darin, ein RSA-Schlüsselpaar entweder über PuTTY oder die Linux-Shell zu generieren. Anschließend muss der öffentliche Schlüssel von der AMP Private Cloud Appliance hinzugefügt und als vertrauenswürdig eingestuft werden.

Generieren eines RSA-Schlüsselpaars mit PuTTY

Schritt 1: Stellen Sie sicher, dass Sie PuTTY vollständig installiert haben.

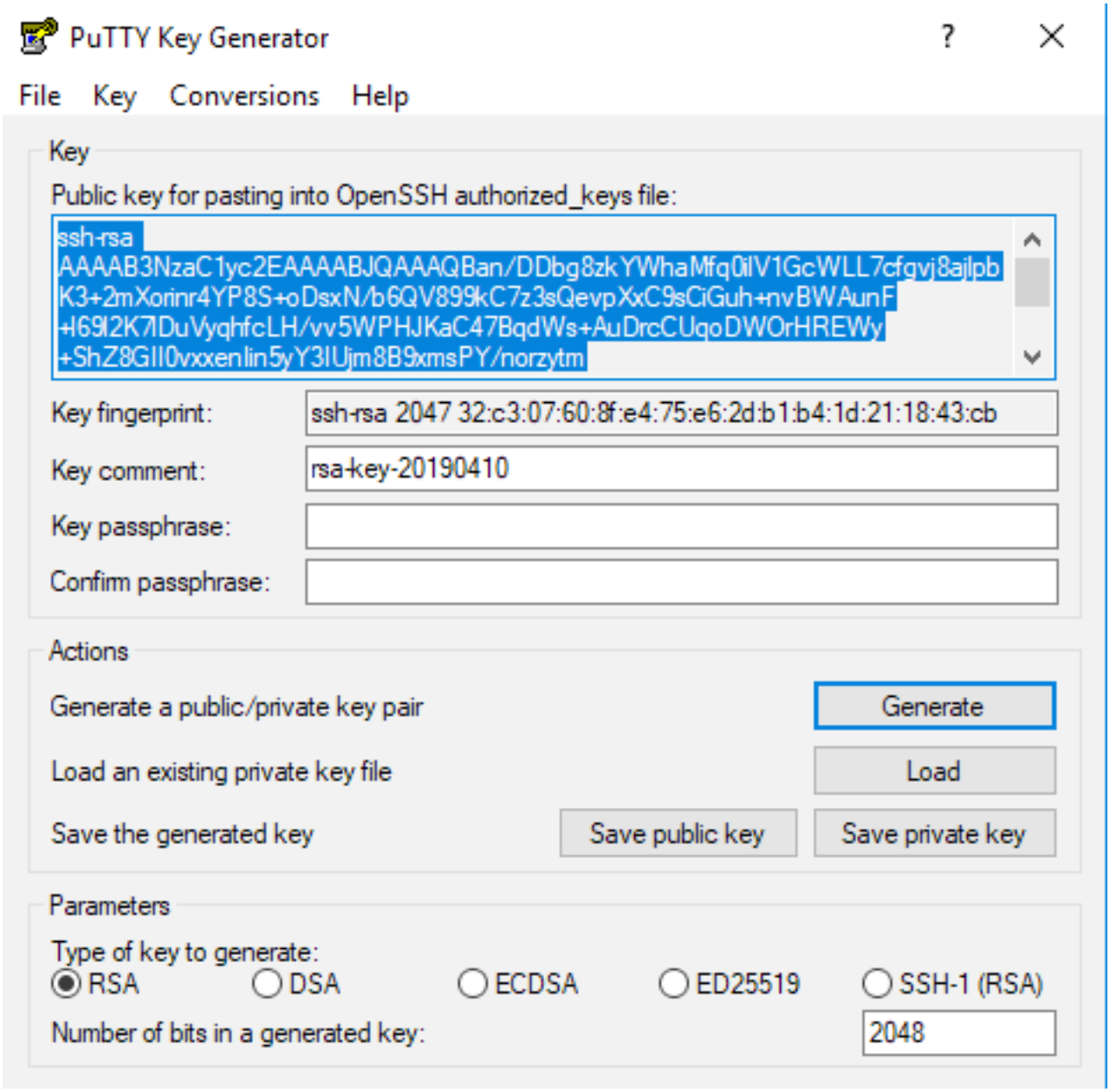
Schritt 2: Starten Sie PuTTYGen, das zusammen mit PuTTY installiert wird, um das RSA-Schlüsselpaar zu generieren.



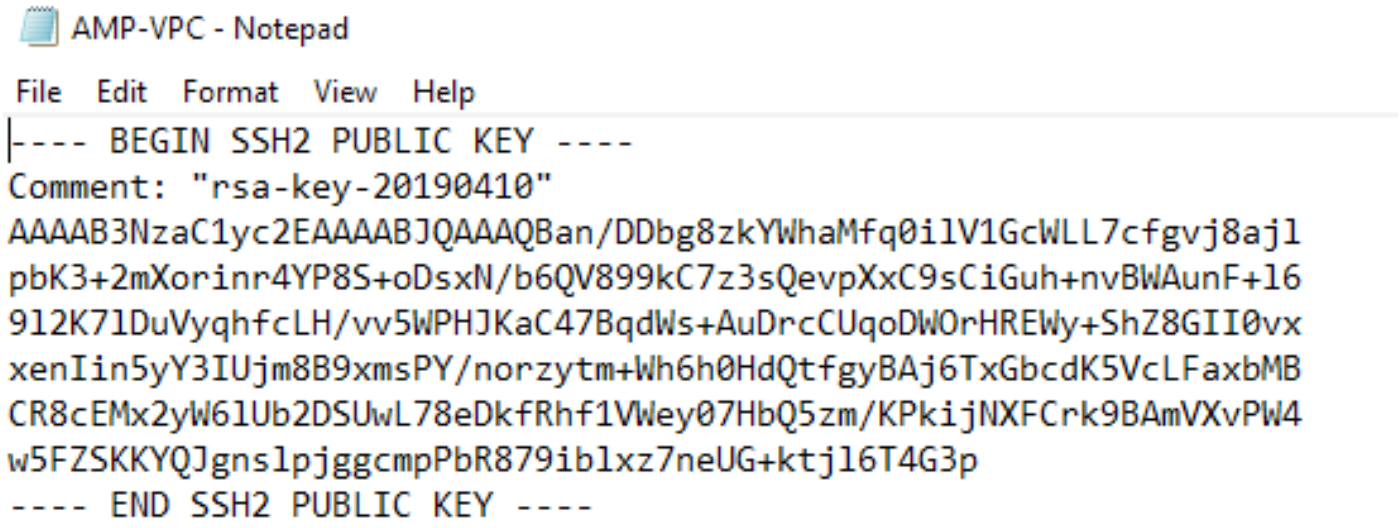
Schritt 3: Klicken Sie auf Generate (Generieren), und bewegen Sie den Cursor zufällig, um die Generierung des Schlüsselpaars abzuschließen.

Schritt 4: Wählen Sie "Save public key" (Öffentlichen Schlüssel speichern) und "Save private key" (Privater Schlüssel speichern), der in den nachfolgenden Abschnitten verwendet werden soll, wie

im Bild hier gezeigt.



Schritt 5: Öffnen Sie den öffentlichen Schlüssel mit Notepad, da das Format geändert werden muss, damit er im AMP Private Cloud Administration Portal akzeptiert werden kann.



Schritt 6: Entfernen Sie die ersten beiden Zeilen, die mit "—BEGIN" beginnen, und die letzte Zeile, die mit "— END" beginnt.

Schritt 7: Entfernen Sie alle Zeilenumbrüche, um den Inhalt des öffentlichen Schlüssels als eine durchgehende Leitung zu gestalten.

Schritt 8: Geben Sie am Anfang der Datei das Wort "ssh-rsa" ein. Speichern Sie die Datei.

RSA-Schlüsselpaar mit Linux/Mac erstellen

Schritt 1: Geben Sie in der Linux/Mac-CLI den Befehl "ssh-keygen" ein.

Schritt 2: Geben Sie die erforderlichen Parameter ein, und dieses erzeugt das RSA-Schlüsselpaar im Ordner "~/.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/w2ll/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$
```

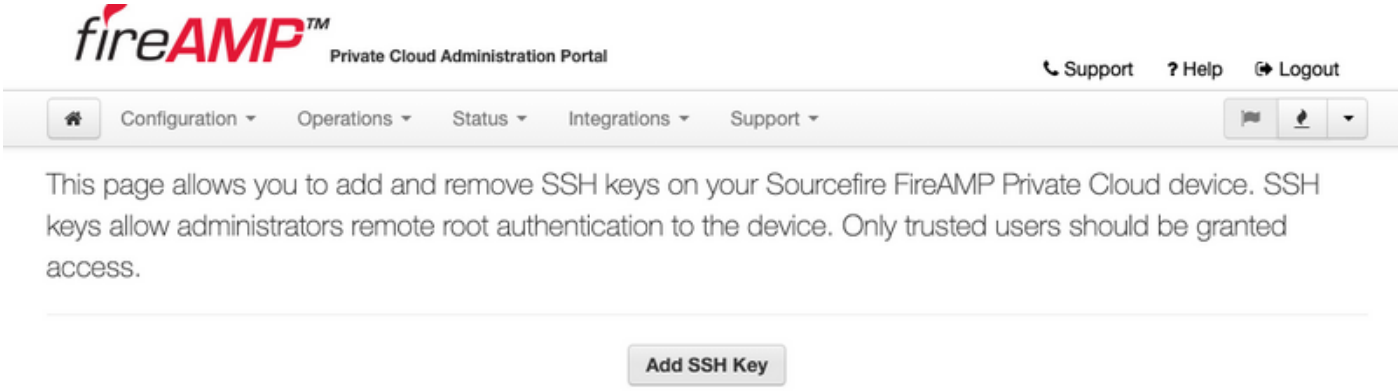
Schritt 3: Wenn Sie den Inhalt von id_rsa.pub öffnen, der der öffentliche Schlüssel ist, können Sie sehen, dass er bereits im erforderlichen Format ist.

```
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 AAAAB3NzaC1yc2EAAAADAQABAAABAQD12Brou9ABf5tLpZKZpF/nPxTnvs9I6cKC+tycnzC6iR1BT/zmqJ
5SVCSmdhnbwOD9cbWzQ7RYgI46SFLa3JeFU11jFzSmAWqI94AHAjFHVp3W5idcZeq9xxsvSm9Z/NPD+roDEGLnRY+y
VMT2wrHGEyxNyWZ0ZLO4Vetmfqof1nx8ixIq+5SwXRdJGFsBNWF0hh8v5rhbxk1ByTVcqGYL3P4JCfMth4tCQDyPd/
CWAlA/263oVDwS4eWEL7haZS+zsqGytOvrNpHnMeoHbc23LKwiFv1xQFy7WFDmxIAGiELVRAKqsv//onbHz/zG/K2J
UL/grTai5amOFq7f2njp abhsha@ABHSHA-M-23ZS
ABHSHA-M-23ZS:.ssh abhsha$
```

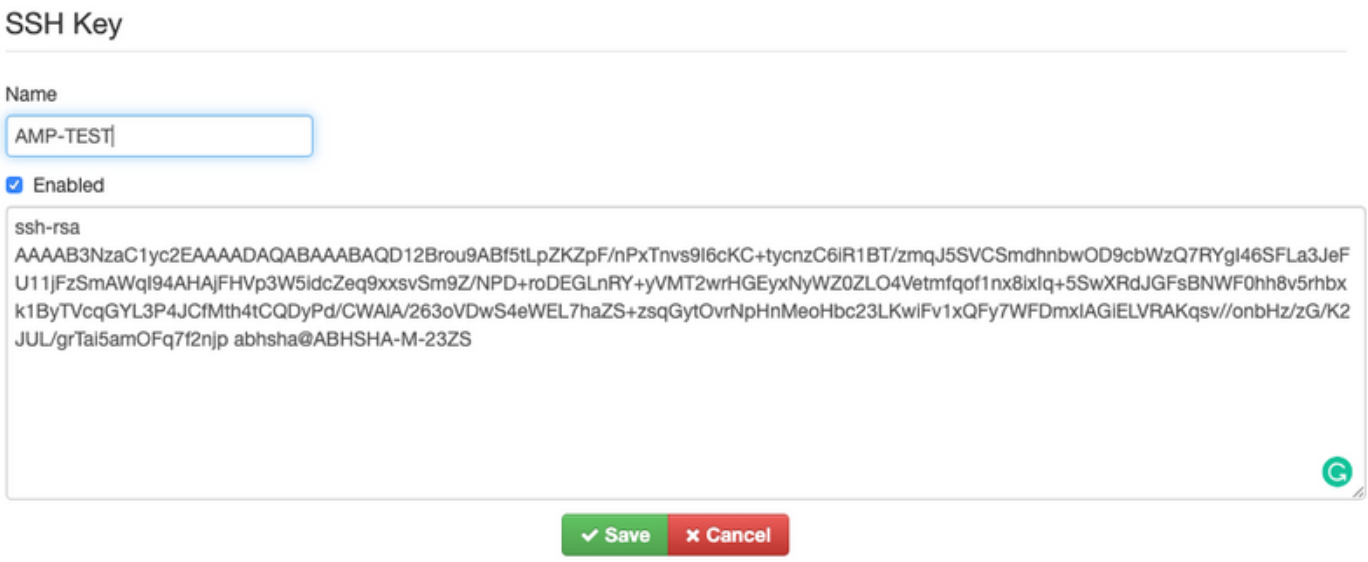
Hinzufügen der generierten öffentlichen Schlüssel zum AMP Private Cloud Administration Portal

Schritt 1: Navigieren Sie zum AMP Private Cloud Administration Portal > Configuration > SSH.

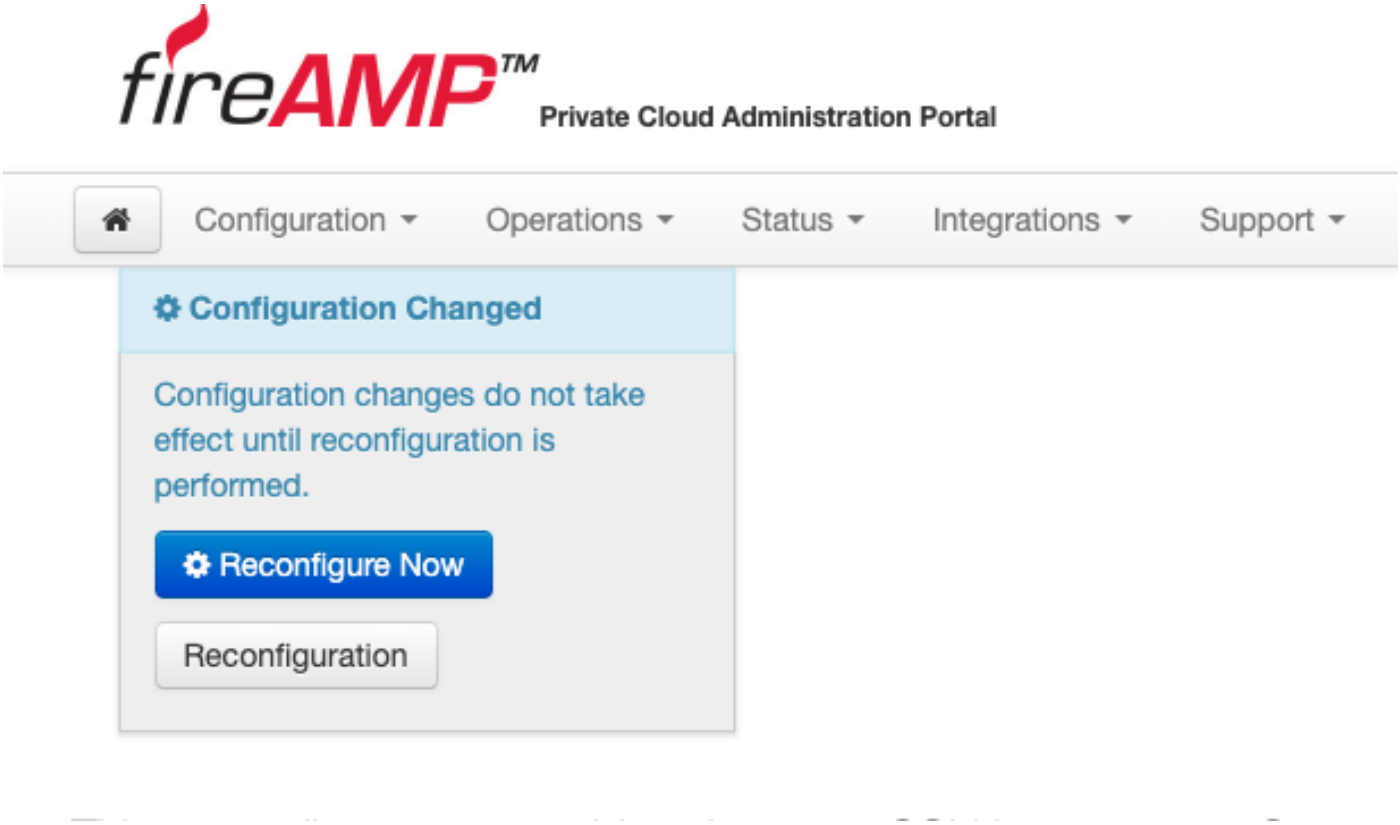
Schritt 2: Klicken Sie auf "SSH-Schlüssel hinzufügen".



Schritt 3: Fügen Sie den Inhalt des öffentlichen Schlüssels hinzu, und speichern Sie diesen.

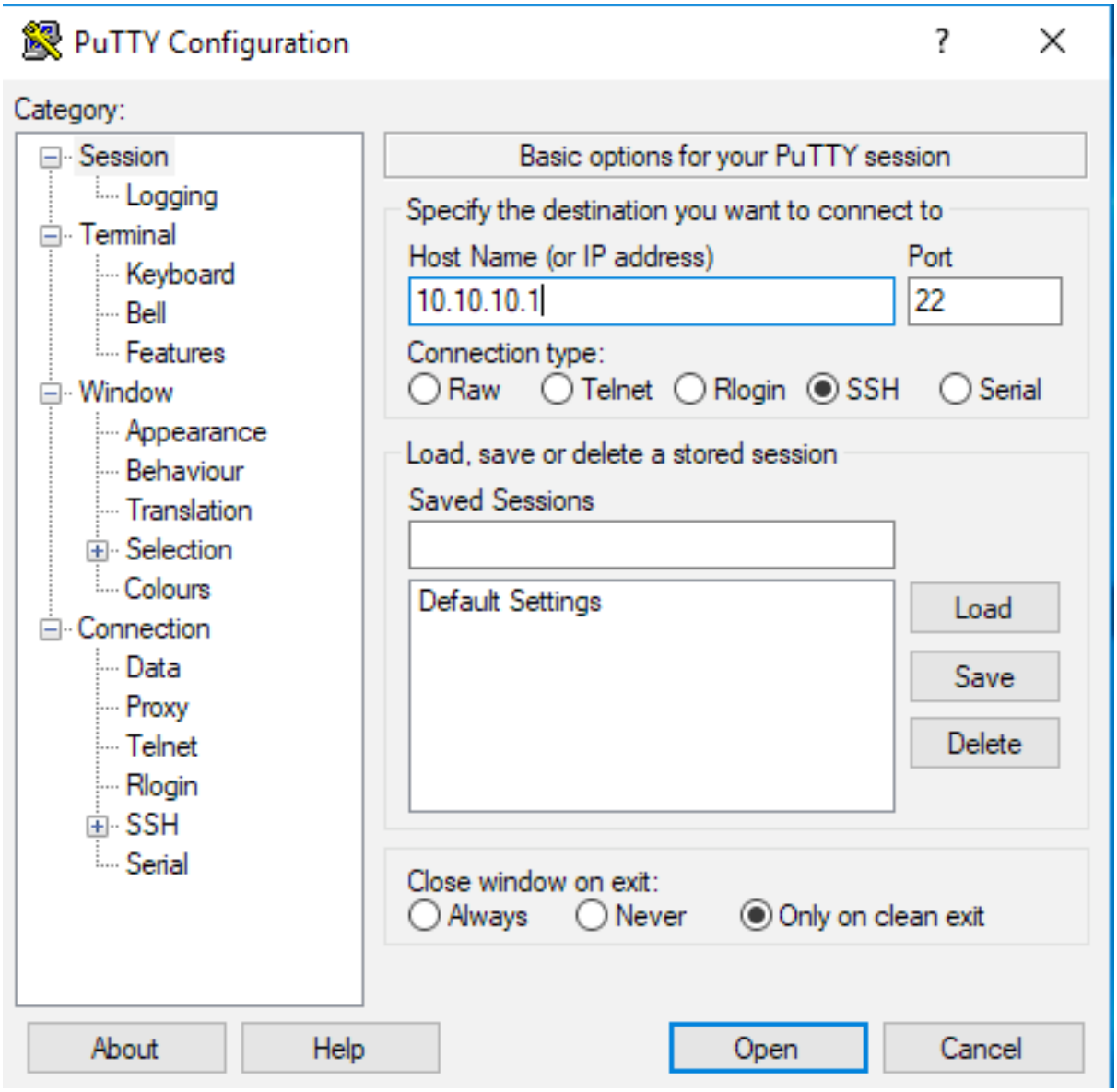


Schritt 4: Nachdem dies gespeichert wurde, stellen Sie sicher, dass Sie die Appliance neu konfigurieren.



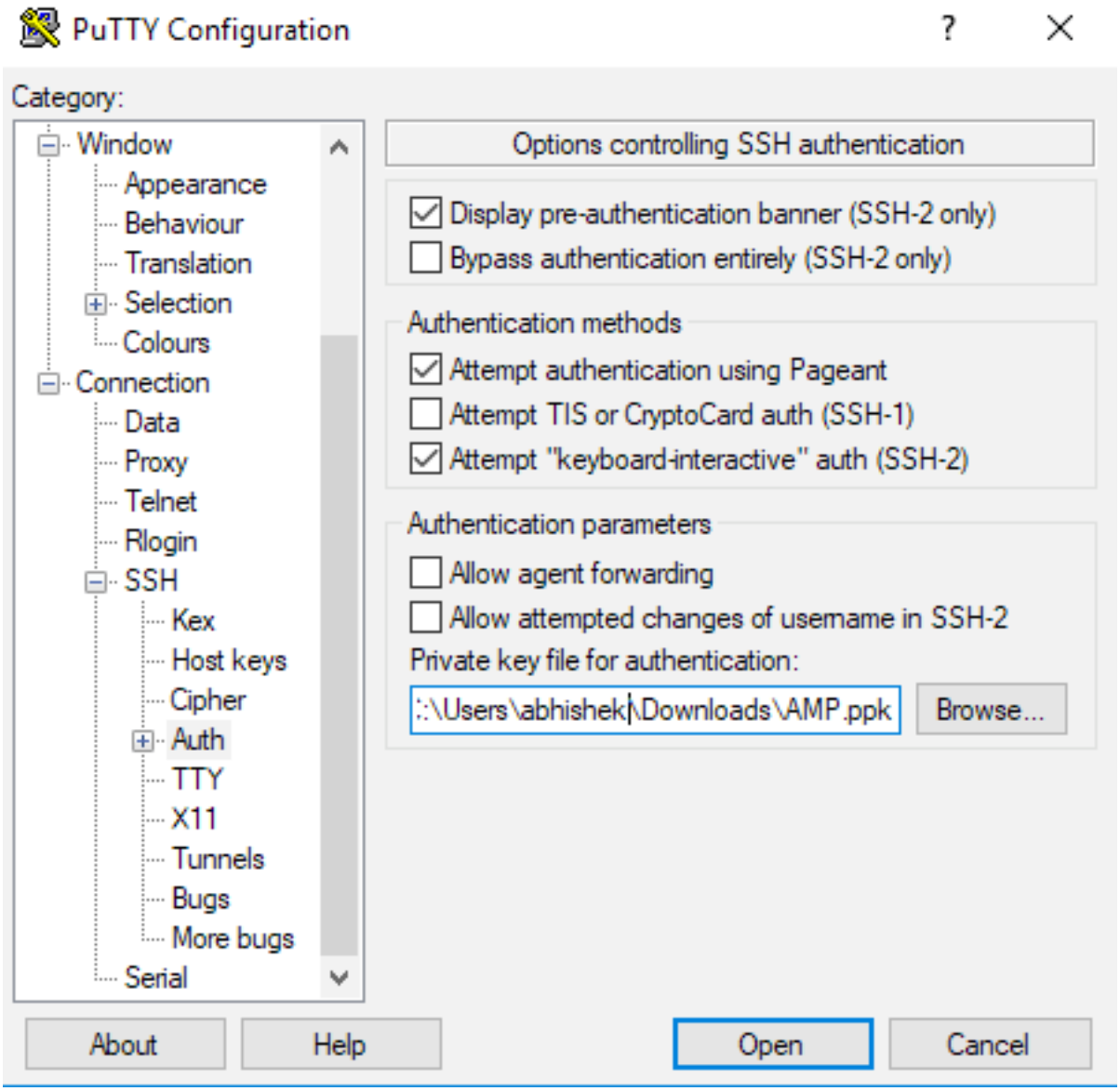
Verwenden Sie das generierte Schlüsselpaar zur SSH-Eingabe in die Appliance mithilfe von PuTTY.

Schritt 1: Öffnen Sie PuTTY, und geben Sie die IP-Adresse des AMP Private Cloud Administration-Portals ein.



Schritt 2: Wählen Sie im linken Teilfenster Connection > SSH aus, und klicken Sie auf Auth.

Schritt 3: Wählen Sie den privaten Schlüssel aus, der von PuTTYGen generiert wurde. Dies ist eine PPK-Datei.



Schritt 4: Klicken Sie auf "Öffnen". Wenn Sie zur Eingabe eines Benutzernamens aufgefordert werden, geben Sie "root" ein. Sie sollten dann in der CLI der AMP Private Cloud landen.

Verwenden des konfigurierten Schlüsselpaars für SSH in die Appliance unter Linux

Schritt 1: Wenn die privaten und öffentlichen Schlüsselpaare korrekt im Pfad " ~/.ssh" gespeichert sind, sollten Sie in der Lage sein, SSH zur AMP Private Cloud-Appliance zu senden, indem Sie einfach den Befehl ssh eingeben, ohne Sie zur Eingabe eines Kennworts aufzufordern.

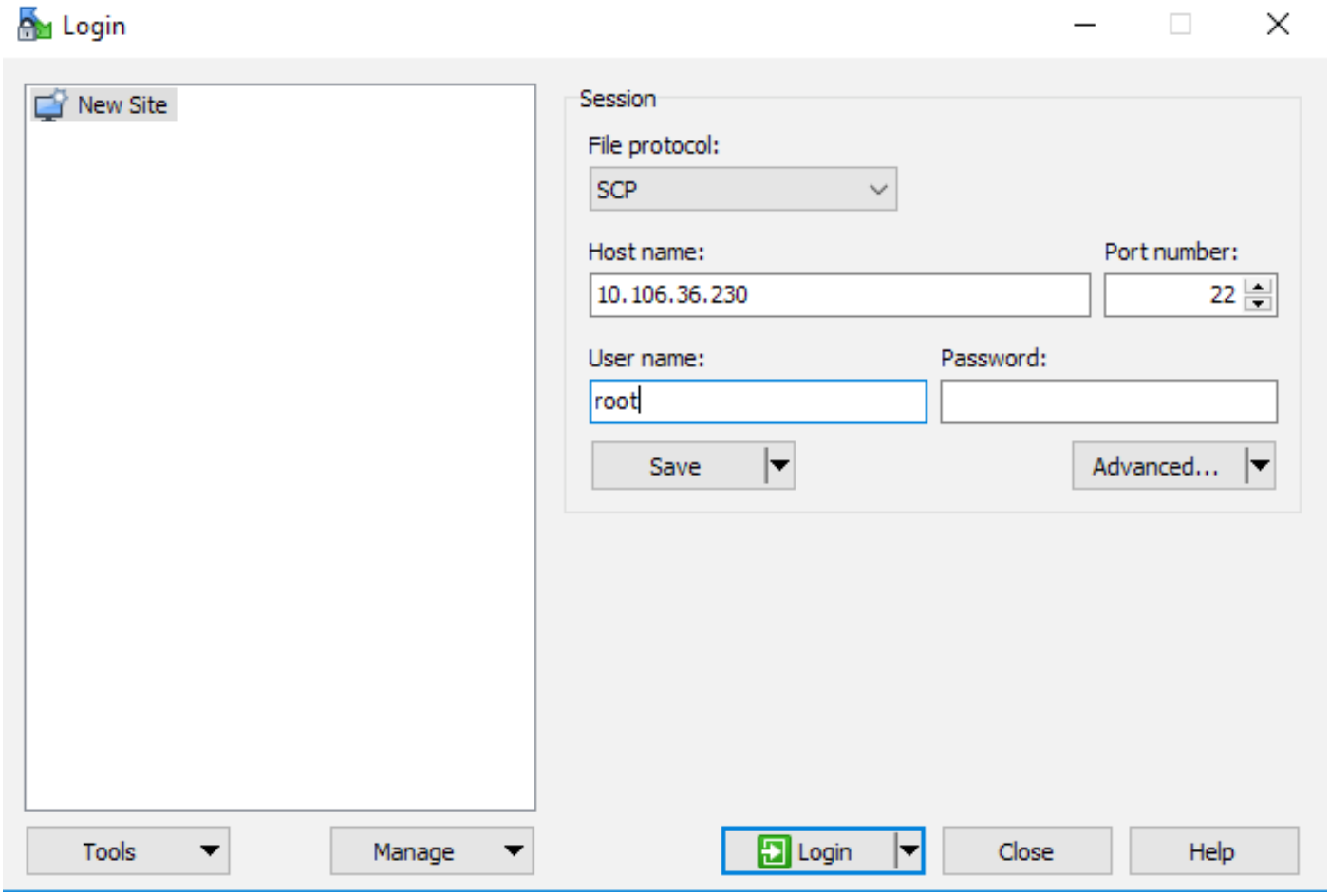
ssh root@<AMP-IP-ADDRESS>

```
[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 ~]#
```

Verwenden von WinSCP für die Interaktion mit dem Dateisystem der AMP Private Cloud

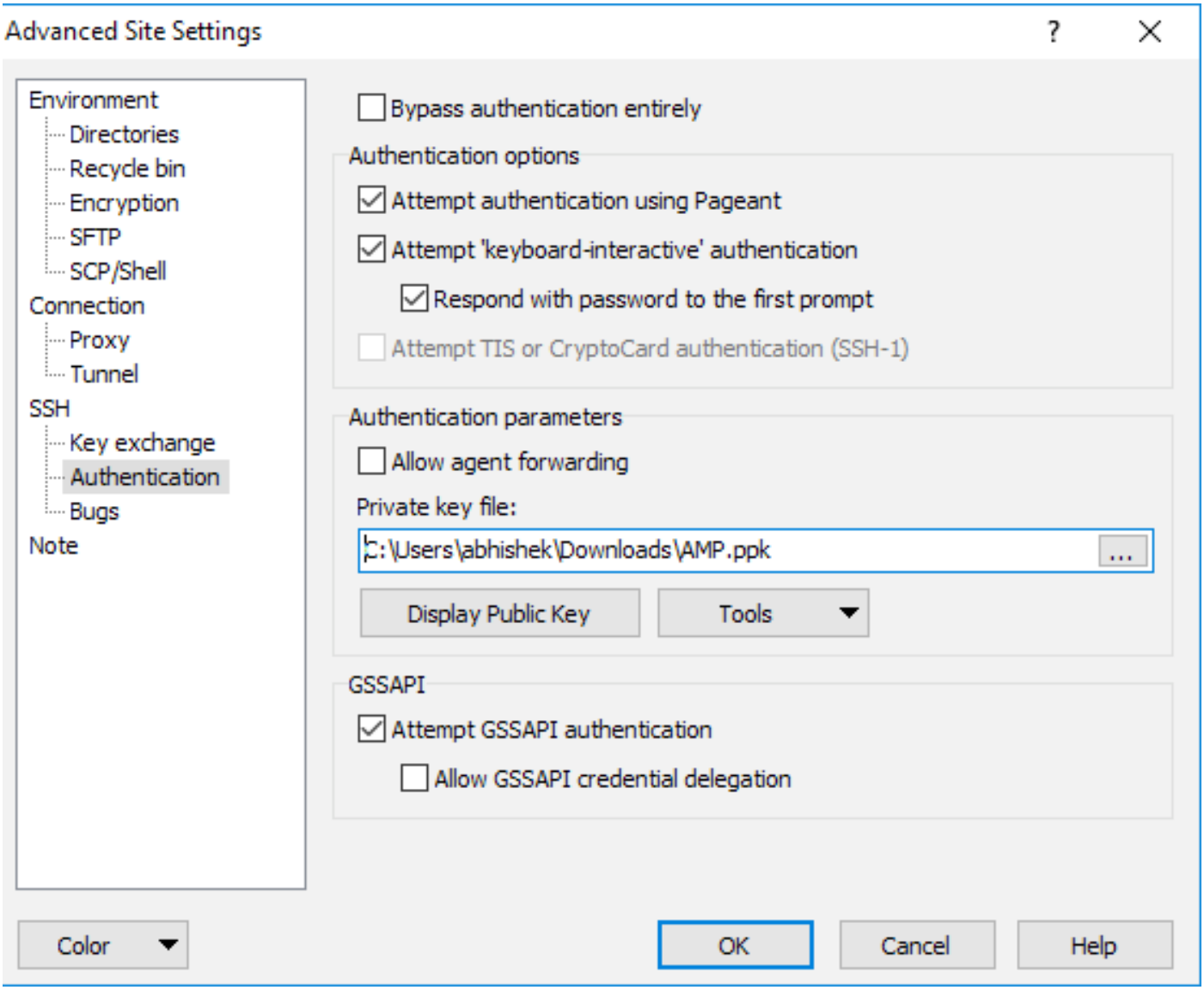
Schritt 1: Installieren Sie WinSCP auf Ihrem Computer, und starten Sie es.

Schritt 2: Geben Sie die IP-Adresse des AMP Private Cloud Administration-Portals ein, und wählen Sie das Dateiprotokoll als SCP aus. Geben Sie den Benutzernamen als root ein, und lassen Sie das Kennwortfeld.



Schritt 3: Wählen Sie Advanced > Advanced > SSH > Authentication aus

Schritt 4: Wählen Sie die PPK-Datei aus, die von PuTTYgen als privater Schlüssel generiert wurde.



Schritt 5: Klicken Sie auf OK und anschließend auf Anmelden. Sie sollten sich erfolgreich anmelden können, nachdem Sie die Aufforderung akzeptiert haben.