**问题：**

SSH 连接时提示 does not support diffie-hellman-group1-sha1 for keyexchange 或 The negotiation of encryption algorithm is failed

**解决方法：**

使用老版本的SSH客户端链接使用最新版的SSH服务的服务器时，经常会遇到 does not support diffie-hellman-group1-sha1 for keyexchange 或 The negotiation of encryption algorithm is failed 错误，因为客户端使用的协议在最新版的SSH中已经不支持了。

有两种解决方法：第一种当然是升级您的SSH客户端，第二种就是修改SSH服务的配置，让其支持客户端使用的协议。这里介绍的是第二种解决方法。

首先在SSH服务器的配置文件 /etc/ssh/sshd\_config 中加入一行如下代码：

|  |  |
| --- | --- |
|  | KexAlgorithms diffie-hellman-group1-sha1,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1 Ciphers 3des-cbc,blowfish-cbc,aes128-cbc,aes128-ctr,aes256-ctr |

保存后，在执行语句：

|  |  |
| --- | --- |
|  | ssh-keygen -A |

最后重启SSH服务：

|  |  |
| --- | --- |
|  | service ssh restart |