

AWS 虚拟机 pem 密钥的使用

在 aws 云上创建虚拟机时都会要求我们选择一个密钥对文件，或生成一个。以后登录虚拟机就得用相应的 pem 密钥对文件，如果是 windows 系统，则要求使用此 pem 文件获取登录密码，如果是 Linux 系统，则要求使用此 pem 文件登录，就是在 ssh 登录时指定以密钥文件登录。

①登录 windows 系统

首先在 EC2 控制面板里选择要登录的虚拟机，再点击上边的“连接”，弹出“连接到您的实例”对话框，连接方法为“一个独立的 RDP 客户端”，中间是虚拟机的公有 ip 信息及登录用户名，点击“获取密码”



在“密钥对路径”这里，点击“Browse”，选择我们之前下载到电脑上的密钥对文件



最后点击解密密码，可得登录密码，如下图：

连接到您的实例

连接方法

☒ 一个独立的 RDP 客户端 

☐ 会话管理器 


要连接至 Windows 实例，您可以使用自选的远程桌面客户端，并下载和运行以下 RDP 快捷方式文件：

下载远程桌面文件

收到系统提示时，请使用以下详细信息连接至您的实例：

公有 IP 

用户名 Administrator

密码 

如果您已将自己的实例加入目录，便可使用目录证书连接到您的实例。

如果您需要连接到实例方面的帮助，请参阅我们的“[链接文档](#)”。

关闭

记住登录 ip 和用户名后，复制密码，关闭此对话框，就可以用 mstsc 远程桌面登录虚拟机了。

②登录 Linux 系统

在 linux 系统客户端若要登录 目标虚拟机，使用 xxx.pem 密钥对文件登录，使用以下命令：

```
ssh -i xxx.pem root@x.x.x.x
```

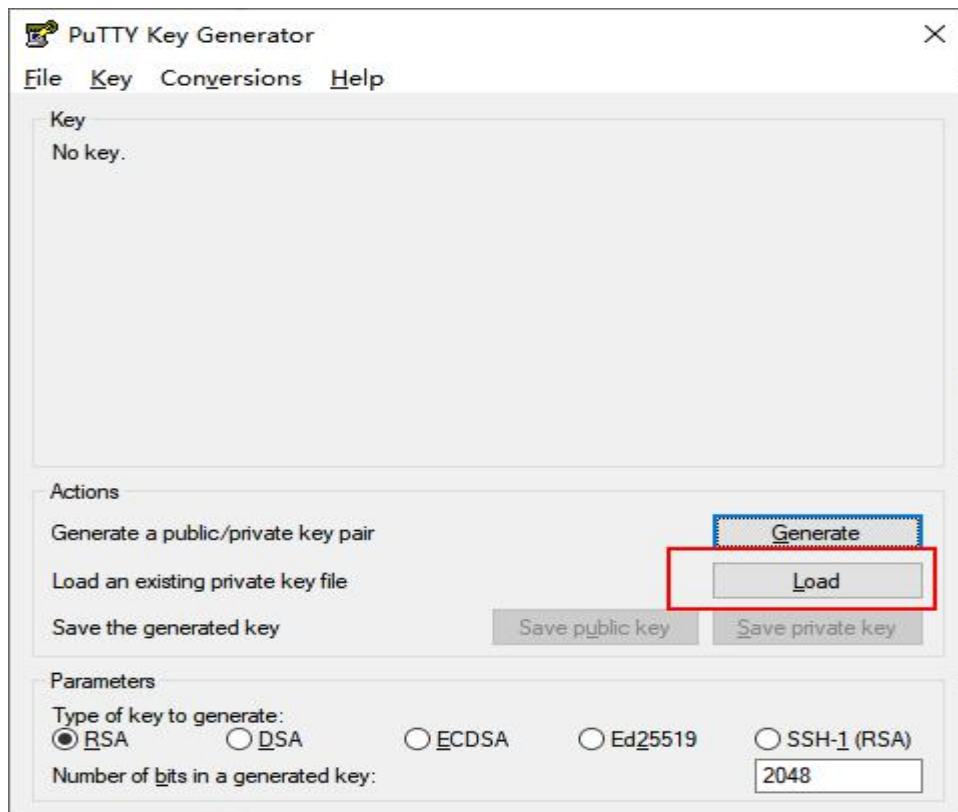
在 windows 上登录 linux 可用其他虚拟终端软件，比如 Putty:



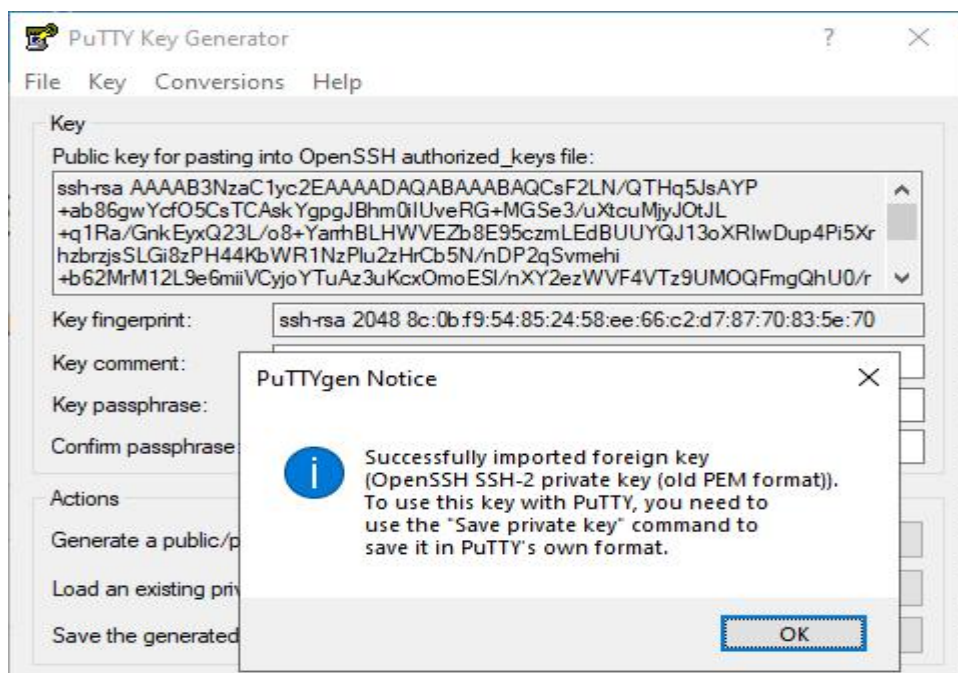
首先打开 puttyGen.exe，把.pem 文件格式转为 putty 的密钥文件格式，xxx.pem 密钥对文件就是 rsa 算法生成的一个密钥对文件，使用 base64 编码，putty 登录 linux 时要使用的密钥为其中的公钥还是私钥，我们暂不知道，因为虚拟机那边是用哪个进行加密的，不确定，所以我们导出 putty 专用的密钥文件，最好是导出 private key，因为私钥文件里也是包含有公钥的。putty 的密钥文件后缀为.ppk

putty 下载地址：<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

下载安装版的，才有 puttyGen.exe 程序

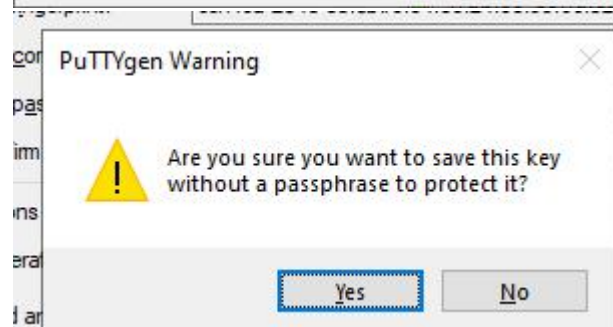
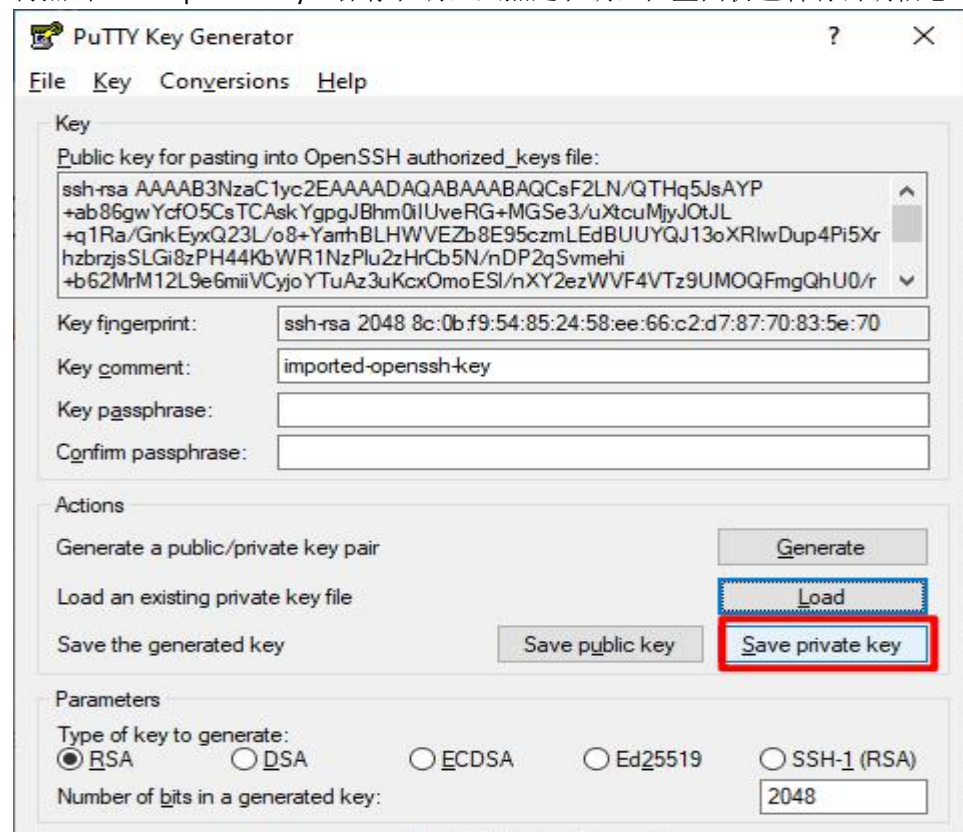


如上图，打开 puttyGen.exe 后，点击“Load”导入，导入文件类型为 All Files(*.*)，再找到之前下载到电脑上的 xx.pem 密钥对文件，

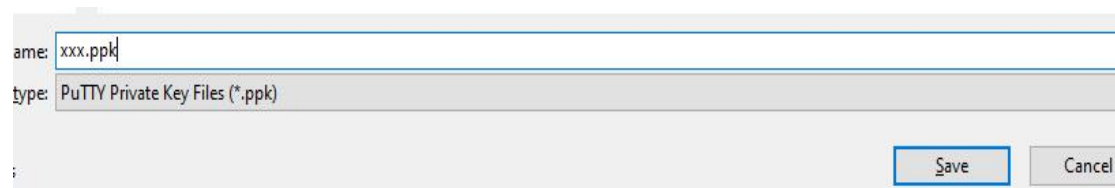


打开之后，提示导入成功，点击 OK

再点击“Save private key”保存私钥，虽然是私钥，但里面仍包含有公钥信息



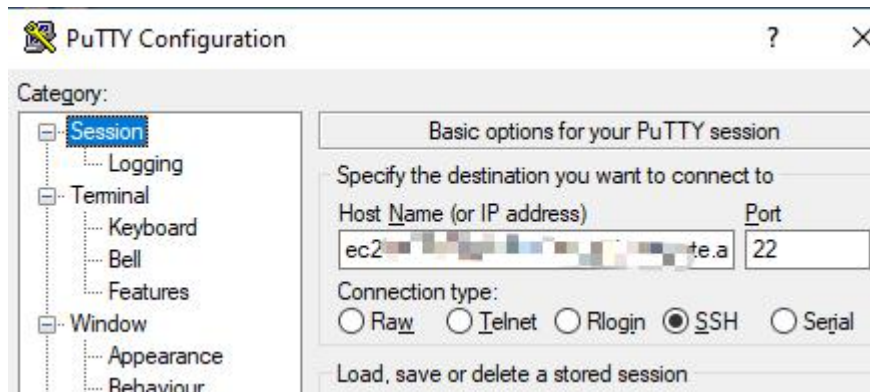
点击“Yes”，输入保存的文件名，后缀为.ppk



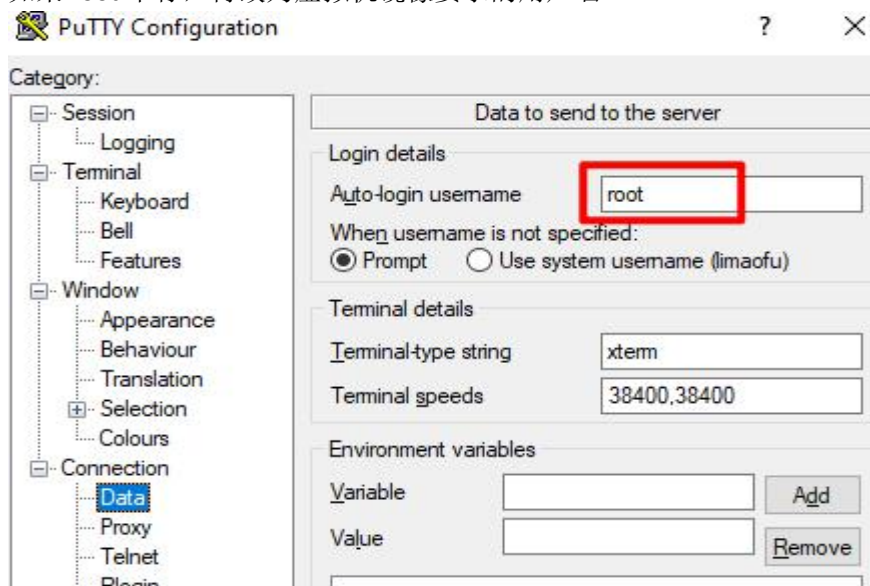
转换完成后，就可以打开 putty.exe



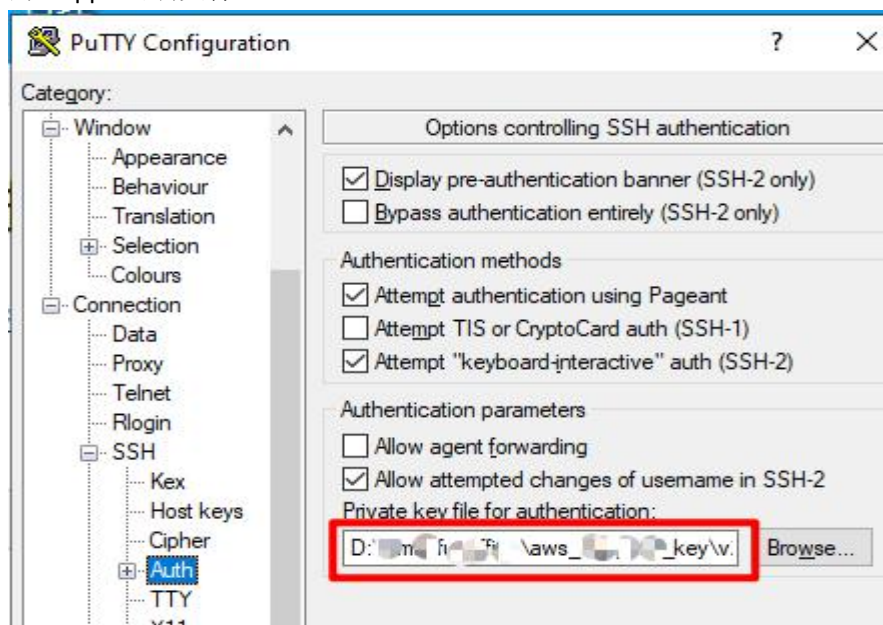
先在 Session 栏里输入 HostName，Port



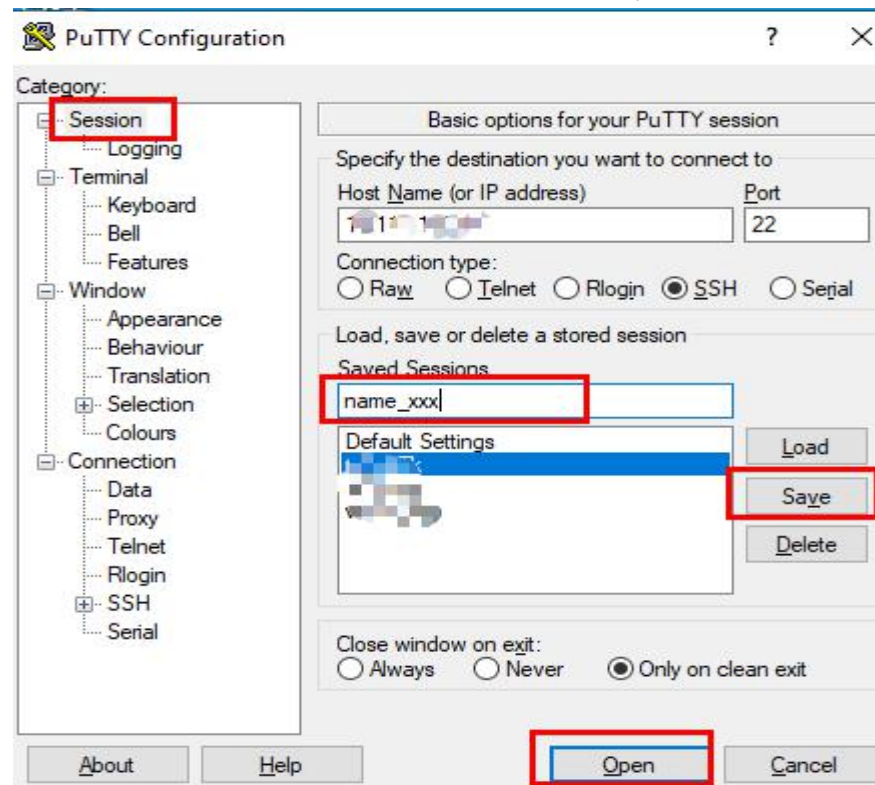
再点击 Connection 下的 Data，在右边 Auto-login username 栏输入用户名，一般为 root
如果 root 不行，再改为虚拟机镜像要求的用户名



再点击 Connection→SSH 下的 Auth，右边的 Private key file for authentication 里选择刚刚转换的 xx.ppk 密钥文件



最后就可以回到 Session，进行保存会话，再点击 Open 打开连接。



Cof-Lee
2020-09-04