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"



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 (i)

 〇会话管理器 (i)

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:

×

关闭

下载远程桌	真面文件
收到系统提示时,请使用以下详细信息连接至您的实例	J:
公有 IP 1	are weather a section of the
用户名 Adr	ninistrator
密码 一时	sodVq ;
如果您已将自己的实例加入目录,便可使用目录证书道如果您需要连接到实例方面的帮助,请参阅我们的"链	E接到您的实例。 接文档"。

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私钥,因为虚拟机那边(目标服务器)使用的是公 钥,所以我们要导出的是 private key。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

-	uiii									>
le	<u>K</u> ey	Conve	rsions	<u>H</u> elp						
Ke	y									
No	key.									
Act	tions									
Act Ge	tions	a public/	private ke	ey pair				(<u>G</u> enerate	
Act Ge	tions nerate ad an e	a public/ xisting pr	private key	ey pair file			ſ		<u>G</u> enerate Load	
Act Ge Lo: Sa	tions nerate ad an e ve the p	a public/ xisting pr generate	private ke ivate key d key	ey pair file		Sav	e p <u>u</u> blic key	Savi	<u>G</u> enerate Load e private key	
Act Ge Lo: Sa Par	tions nerate ad an e ve the p rameter	a public/ xisting pr generate s	private ke ivate key d key	ey pair file		Save	e p <u>u</u> blic key	Sav	<u>G</u> enerate Load e private key	
Act Ge Loa Sa Par Tyr	tions nerate ad an e ve the rameter pe of ke <u>R</u> SA	a public/ xisting pr generate s s ey to gen (private key ivate key d key erate: ◯ <u>D</u> SA	ey pair file	⊖ <u>e</u> cds	Sav	e public key	Sav	<u>G</u> enerate Load e private key) SSH- <u>1</u> (RSA)	

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,

✓ All Files (*.	*) ~	
打开(0)	▼ 取消	
PuTTY Key Genera	itor	7 >
Kev	ins Heip	
Public key for pasting	into OpenSSH authorized keys file	
ssh+sa AAAAB3Nza +ab86gwYcfO5CsTC +q1Ra/GnkEyxQ231 hzbrzjsSLGi8zPH44 +b62MrM12L9e6mii\	CTyc2EAAAADAQABAAABAQCsF2 AskYgpgJBhm0iIUveRG+MGSe3/ ./o8+YamhBLHWVEZb8E95czmLE &WR1NzPlu2zHrCb5N/nDP2qSvn /CyjoYTuAz3uKcxOmoESI/nXY2ez	2LN/QTHq5JsAYP wXtcuMjyJQtJL dBUUYQJ13oXRIwDup4Pi5Xr nehi WVF4VTz9UMOQFmgQhU0/r
Key fingerprint:	ssh-rsa 2048 8c:0b:f9:54:85:24:	58:ee:66:c2:d7:87:70:83:5e:70
Key comment: Key passphrase:	PuTTYgen Notice	×
Confirm passphrase	OpenSSH SSH-2 priva	I foreign key ate key (old PEM format)).
Generate a public/p	use the "Save private save it in PuTTY's own	key" command to n format.
Load an existing priv		
Save the generated		ОК

打开之后,提示导入成功,点击 OK

冉忠山 Save private key 不住心	冉点击	"Save private key"	保仔私钥
--------------------------	-----	--------------------	------

PuTTY Key Genera	tor		?	×
ile <u>K</u> ey Con <u>v</u> ersio	ns <u>H</u> elp			
Key		2		12
Public key for pasting	into OpenSSH authorized_keys fil			-
+ab86gwYcf05CsTC +q1Ra/GnkEyxQ23L hzbrzjsSLGi8zPH44K +b62MrM12L9e6miiV	, IyozzaAAAADAQABAAABAQCsF AskYgpgJBhm0ilUveRG+MGSe3 /o8+YanhBLHWVEZb8E95czmL bWR1NzPlu2zHrCb5N/nDP2qSv CyjoYTuAz3uKcxOmoESI/nXY2e	2LIV/Q1Hq5JsATP //uXtcuMjyJOtJL EdBUUYQJ13oXRIwDu /mehi zWVF4VTz9UMOQFmg	up4Pi5Xr jQhU0/r	
Key fingerprint:	ssh-rsa 2048 8c:0b:f9:54:85:24	:58:ee:66:c2:d7:87:70:	83:5e:70	
Key <u>c</u> omment:	imported-openssh-key			
Key p <u>a</u> ssphrase:				
Confirm passphrase:				
Actions				
Generate a public/priv	vate key pair	Ge	enerate	
Load an existing priva	te key file		<u>L</u> oad	
Save the generated k	ey Save	p <u>u</u> blic key <u>S</u> ave	private ke	y
Parameters				
Type of key to genera	te:			
Number of hits in a ge	DSA <u>C</u> CDSA		19	
Humber of <u>b</u> its in a ge	notaca key.			
PuTTYgen Warning		×		
E				
Are you s without a	ure you want to save this key a passphrase to protect it?			
r	Yes <u>N</u> o			
、击"Yes",输入伤	R存的文件名,后缀为.ppk			
e: xxx.ppk				
e: PuTTY Private Key Files (*.pp	k)			
				Save

转换完成后,就可以打开 putty.exe



先在 Session 栏里输入 HostName, Port

🕵 PuTTY Configuration	n ?	×
Category:		
E- Session	Basic options for your PuTTY session	i(
Logging ⊡ Terminal Keyboard Bell	Specify the destination you want to connect to Host Name (or IP address) Port ec2 Port	t
Features	Connection type: ○ Ra <u>w</u> ○ <u>T</u> elnet ○ Rlogin ● <u>S</u> SH () Se <u>r</u> ial
Appearance	Load, save or delete a stored session	

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

	PuTTY Configuration	
--	---------------------	--

? X

Login details Auto-login usemame Whe <u>n</u> usemame is not s Prompt OUse sy	pecified: specified: ystem username (limaofu)
Terminal details	
Terminal-type string	xterm
Terminal speeds	38400,38400
Environment variables	
<u>V</u> ariable	Add
Value	Remov
	Login details Auto-login usemame When usemame is not s Prompt Use sy Terminal details Ierminal-type string Terminal speeds Environment variables Variable Value

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



	?
Basic options for your PuTTY	session
Specify the destination you want to con Host <u>Name</u> (or IP address)	nect to <u>P</u> ort
Connection type: ○ Ra <u>w</u> ○ <u>T</u> elnet ○ Rlogin ● <u>S</u>	SH O Serial
Load, save or delete a stored session Saved Sessions name_xxx Default Settings	load
23 .	Sa <u>v</u> e
Close window on exit:	
	Basic options for your PuTTY Specify the destination you want to con Host Name (or IP address) 1111 Connection type: O Raw O Telnet O Rlogin O S Load, save or delete a stored session Saved Sessions name_xxxl Default Settings Cose window on exit:

最后就可以回到 Session,进行保存会话,再点击 Open 打开连接。

Cof-Lee 更新日期: 2020-12-04