SSH Key Practice

USE CASE we are starting exiting instance with newly generated keys

1. launch instance in gitbash with private key eg abc.pem
2. check the autheration key in your instance$ cd .ssh
3. $ **ls**
4. see content of authorized Key with command$ **cat authorized\_keys**
5. start new session in gitbatch it will be your machine window
6. go to folder where pem file is available eg cd Deskstop
7. create new key pair with **ssh-keygen –o**
8. two file one with extention.pub and one without extension will be created eg xyz.pub and xyz if you do not provide names it will take by default name id\_rsa id\_rsa.pub
9. we can check content that our new key pair is generated by **ls**
10. now we need to send these key on instance
11. scp -i key.pem **newkey which we have createded.pub** ec2-user@instancepublicip://path of ec2 folder/home/ec2-user
12. eg **scp –i abc.pem xyz.pub ec2-user@instancepublicip:/home/ec2-user**
13. this will show error but you need to go to instance window and check by ls
14. eg xyz.pub is copied in instance (after checking ls go back to instance ip eg [ec2-user@ip-172-31-3-183 ~])
15. echo \"`cat /home/ec2-user/ **newkey which we have createded.pub** `\" >> .ssh/authorized\_keys
16. eg echo \"`cat /home/ec2-user/ **xyz.pub** `\" >> .ssh/authorized\_keys
17. new window it will be our third window
18. login instance with newkey without extension
19. eg chmod 400 xyz
20. eg ssh –I xyz ec2-user@publicip
21. if you are facing trouble it will be due “” in authorized appended key
22. to solve this
23. follw following step

* sudo vi authorized\_keys
* press I to go in insert mode
* remove double quotes save with :wq
* exit