################ PART II. Pre-requisite

####################### Step 0. Assume that you Setup the 3 machines at Amazon EC2 using the Ubuntu AMI, with the following machine names. I also assume that the same security group and the security keys (machine0.pem) are used for all 3 machines . The following instructions assume the 3 linux instances generated are: machine0, machine1, machine2 with the following matching IP addresses:

52.20.205.45 machine0

52.4.171.43 machine1

52.7.144.47 machine2

####################### Step 1.1 At each machine, Edit the /etc/hosts files so the machine nick name and the IP Address matches up. You can use sudo vi /etc/hosts to add the following and save:

52.20.205.45 machine0

52.4.171.43 machine1

52.7.144.47 machine2

Note: when you 'run ssh machine1', Linux shell will look at /etc/hosts for the matching IP Address.

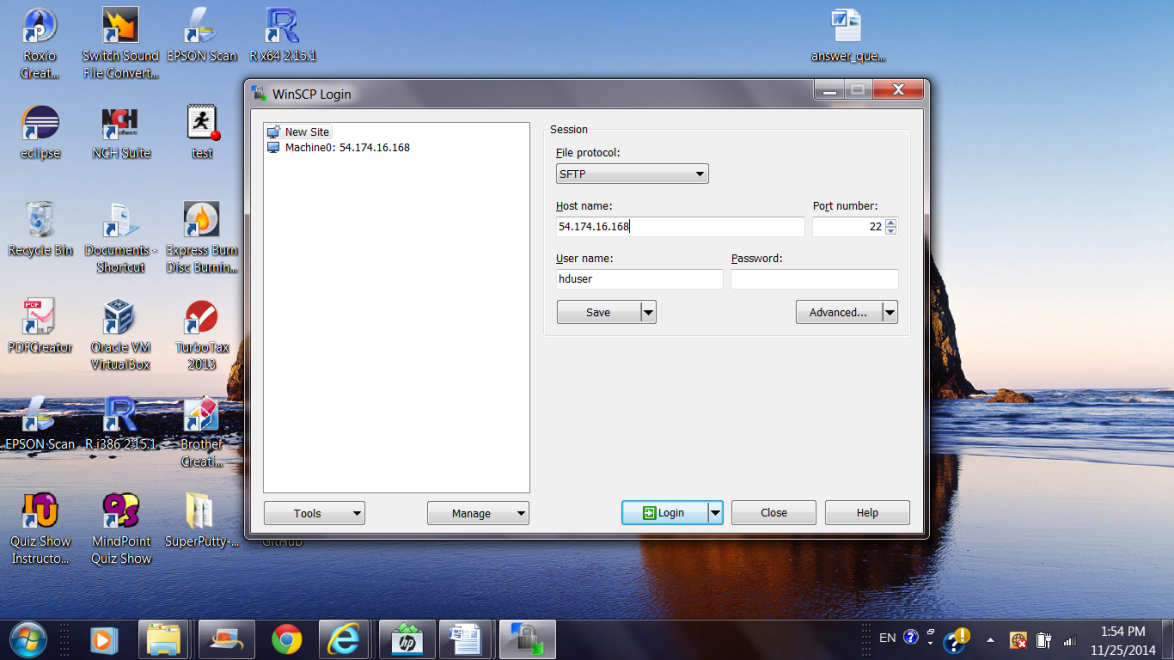
####################### Step 1.2 At each machine, run the following command to change the machine hostname:

sudo hostnamectl set-hostname machine0 #substitue machine1 for machine0 for 2nd machine

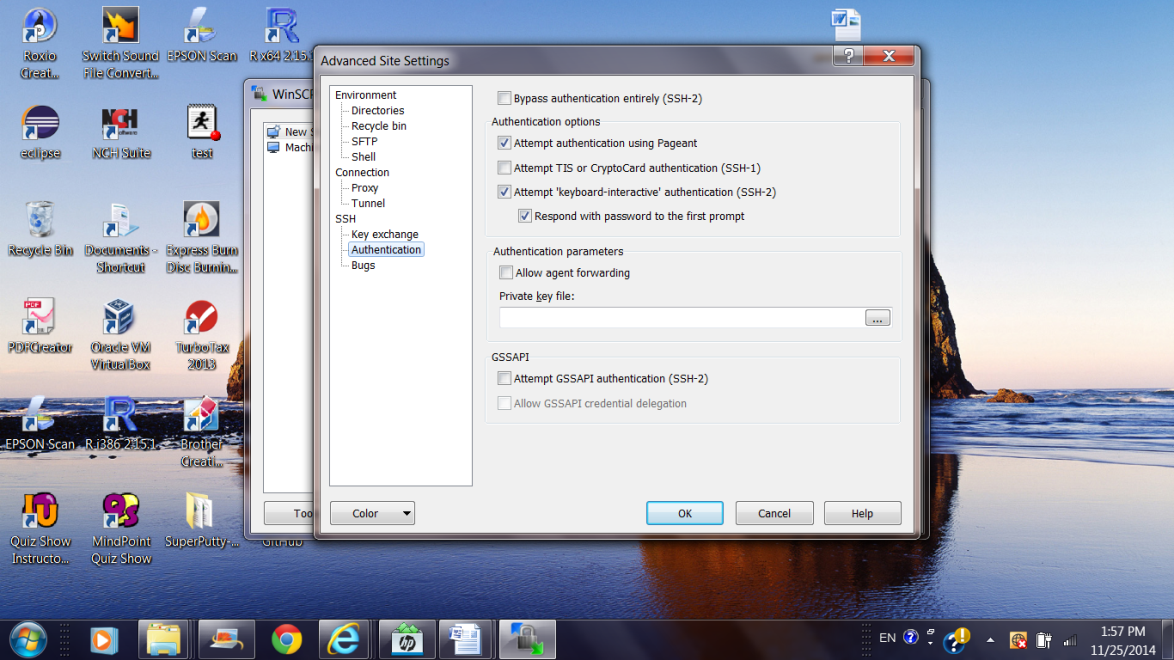
The machine hostname is stored at /etc/hostname. It is shown within your linux prompt such as: "ubuntu@ip-172-31-11-108:~$". Close your Ubuntu session and start a new session, you should see your new prompt should be "ubuntu@machine0:~$".

####################### Step 2. Use WinSCP to copy the key pair file “machine.pem” to the .ssh folder of each machine. You could copy it to one of the machine and then use scp to copy it to the other machines.

####################### Step 2. 1 Open the WinSCP tool. You should see a screen like this.



####################### Step 2. 2 Pick “SCP” function, input the IP address of the machine0, the user ‘ubuntu’, and click on the ‘Advanced’.



####################### Step 2.3 Click ‘SSH’ and ‘Authentication', then open the browser to locate the private key file and input it.

####################### Step 2. 4 Click ‘OK’ and click ‘Login’. You should see a screen. The right-hand-sight of the panel is the folders of your linux instance: machine0 (Yours may have very few items for your own machine!)

## 

####################### Step 2.5 You can use this GUI to copy (click and pull) machine0.pem to the “.ssh” folder of your target machine0. Close the WinSCP session after it's done.

####################### Step 3. Copy the machine0.pem key file to id\_rsa

####################### Step 3.1 At machine0, copy the machine0.pem to id\_rsa, the default remote access code.

mv ~/.ssh/machine0.pem ~/.ssh/id\_rsa

chmod 600 ~/.ssh/id\_rsa

####### With id\_rsa in place, you can run the following to see if it works!

ssh machine1 (or 52.4.171.43) to see if it works.

####### Full version command will be “ssh –i machine0.pem ubuntu@52.4.171.43”

####################### Step 3.2 After keyless “ssh” works at machine0, copy the key file to the folder “.ssh” of the other machines (machine1 and machine2).

scp ~/.ssh/id\_rsa [ubuntu@machine1:/home/ubuntu/.ssh/id](mailto:hduser@ec2-54-174-1-80.compute-1.amazonaws.com:/home/hduser/.ssh/id)\_rsa

scp ~/.ssh/id\_rsa [ubuntu@machine2:/home/ubuntu/.ssh](mailto:hduser@ec2-54-174-1-89.compute-1.amazonaws.com:/home/hduser/.ssh)/id\_rsa

After this you should be able to ssh from one another by referencing the machine host nick name.

ssh machine1 #(from machine0); Use “exit” to return to machine0.

ssh machine2 #(from machine0); Note: hostname at Linux prompt tells you which machine you are running.

This is why we worked on Step 1.2

ssh machine0 #(from machine1) Use “exit” to return to machine0.

ssh machine2 #(from machine1)

ssh machine0 #(from machine2)

ssh machine1 #(from machine2)