Amazon Web Services:

06-10-2019:

Lab-1:

Launch and EC2 Machine

// Steps to create an EC2 machine:

Click on Launch Instance

Select this AMI: "Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-0927ed83617754711 (64-bit x86) / ami-0e175be6acf8b637d (64-bit Arm)**"**

Click on Select to choose the AMI

Select t2.micro free one and Click on "Next: Configure Instance Details"

Select the checkbox: Enable termination protection

Click on "Next: Add Storage"

Leave it as default the root volume: /dev/sda1

Click on "Next: Add Tags" // Important

Click on "Add Tag"

Name: JenkinsLabs-1

Click on "Next: Configure Security Groups"

Select the "Select an **existing** security group**" // default:** sg-0ed14060

Click on "Review and Launch"

Cross verify all the details

Click on "Launch"

// For first time user always use "Create a new key pair"// Don't loose else you can't connect to your EC2 Instance

// For second time user try to use "Choose an existing key pair" // Remember the saved location

// For first time user

// Ask a "key pair name: <ANY-NAME>" // Like: JenkinsLabs-1

// Click on "Download Key Pair"

// A *.pem like "JenkinsLabs-1.pem" will be downloaded

// Save it

Finally Click on "Launch Instances"

Click on "i-03f724096bd013aab**"**

Wait for Status Checks: 2/2

// Done Till here we have successfully Launch our Instances

Lab-2:

How to connect with an EC2 Instances:

// For Windows
Install putty and try it

// For Linux/Ubuntu/ Any Linux
Terminal by default present no extra software required to connect to an EC2 Instance

// For Mac
Default terminal present

// Lets see how to connect in Mac
Go to AWS Management Console
Search your instance: "<INSTANCE-ID> OR INSTANCE_NAME"
Click on "Connect"
First change the mode:
$ chmod 400 JenkinsLabs-1.pem

// Permissions in Linux:
r -> read -> 4
w -> write -> 2
x -> execute -> 1

rwx -> 7

Permissions for any file or dir
**/ | **
rwx. rwx. rwx
user group others

How we can see the permissions:
$ ls -l <file-name>

// To view the default permission of *.pem file
$ ls -l JenkinsLabs-1.pem // 644
-**rw-r--r--**@ 1 javedalam staff 1692 Oct 6 19:00 JenkinsLabs-1.pem

// As per AWS we will have to change the permissions as 400
$ chmod 400 JenkinsLabs-1.pem
$ ls -l JenkinsLabs-1.pem
-r--------@ 1 javedalam staff 1692 Oct 6 19:00 JenkinsLabs-1.pem

// Try to connect an EC2 Instances:
$ pwd
/Users/javedalam/Documents
$ ssh -i "JenkinsLabs-1.pem" ubuntu@ec2-13-127-17-116.ap-south-1.compute.amazonaws.com
Warning: Identity file JenkinsLabs-1.pem not accessible: No such file or directory.
The authenticity of host 'ec2-13-127-17-116.ap-south-1.compute.amazonaws.com (13.127.17.116)' can't be established.
ECDSA key fingerprint is SHA256:Aec/l0iKElq2qNtAwL3/RrU1J7RcAfbXQ9y+7/OuNng.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-13-127-17-116.ap-south-1.compute.amazonaws.com,13.127.17.116' (ECDSA) to the list of known hosts.
ubuntu@ec2-13-127-17-116.ap-south-1.compute.amazonaws.com: Permission denied (publickey).

// Unable to connect why ?? Because "JenkinsLabs-1.pem not accessible" if you are in different location

// Try again:
$ ssh -i "../Downloads/JenkinsLabs-1.pem" ubuntu@ec2-13-127-17-116.ap-south-1.compute.amazonaws.com
OR
$ ssh -i "JenkinsLabs-1.pem" ubuntu@ec2-13-127-17-116.ap-south-1.compute.amazonaws.com

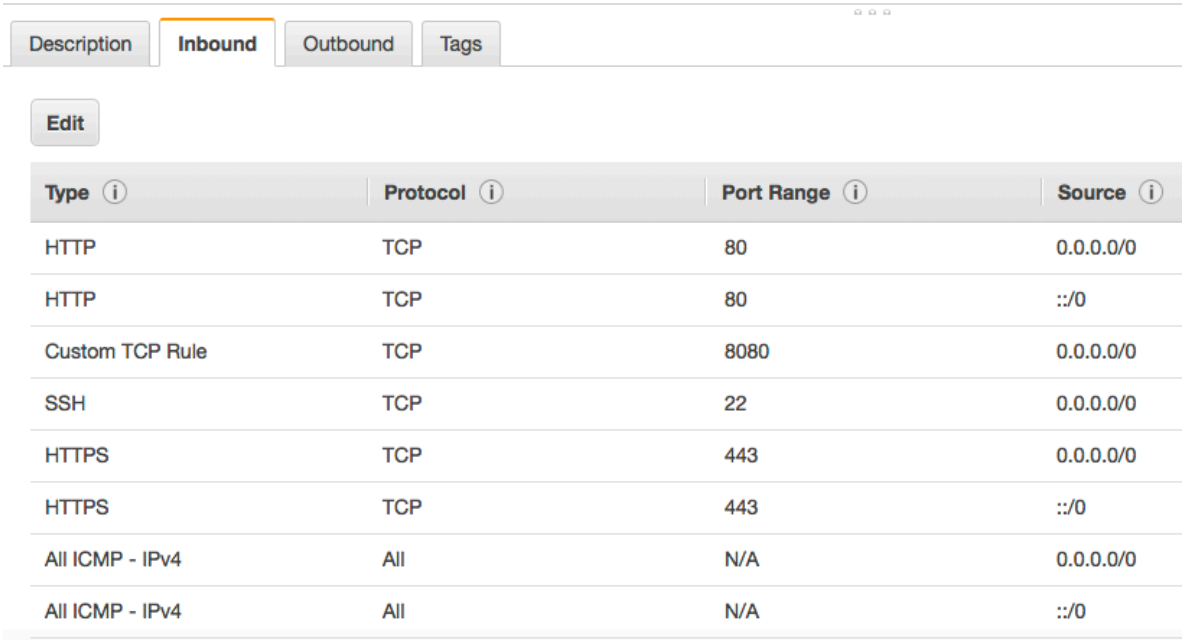
// Successfully Connected with an EC2 Instances

Lab-3:

Add the mandatory SGs

How to add the Security Groups:
// Click on Instance
// Click on "Security Groups" // redirect to SGs page

// Click on Inbound // Incoming requests
// Click on Edit
// Click on Add Rule
// Select the possible option
// Click on Save



Done

Lab-4:

Once activity done always stop the EC2 Instance

// Click on Actions -> Instance Type -> Stop

Green -> Running
Yellow -> Stopping
Red -> Stopped

Logout the Session
