

SSHFS

Secure Shell File System



Video link:

<https://youtu.be/RxmdcL8CVtw>

Prepared by

Balanagameena Nagasubramanian

M.Sc., (Computer Security)

Spring 2020



SUMMARY: This report explains the purpose of SSHFS in ubuntu with an example. (EC2 instance is taken as an example for remote server)

SSHFS: Secure Shell File System

In computing, SSHFS (SSH Filesystem) is a filesystem client to mount and interact with directories and files located on a remote server or workstation over a normal ssh connection. The client interacts with the remote file system via the SSH File Transfer Protocol (SFTP), a network protocol providing file access, file transfer, and file management functionality over any reliable data stream that was designed as an extension of the Secure Shell protocol (SSH) version 2.0.

SSHFS is a mechanism that will support local editing of files without the need to download files to the local system. Simply open and edit your data using your local applications. SSHFS functions well for transferring small (>5GB data files) between the local file system and West Grid file systems.

Task performed here: We are going to mount/place/edit the directory/file in the remote location using SSHFS client through SFTP. It takes in a secure platform. This would be helpful to access and edit the file easily without downloading the file in the local system.

Steps:

1) Create an EC2 instance. An EC2 instance is a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on the Amazon Web Services (AWS) infrastructure.

(Find the screenshots for creating an "AWS EC2 server" in page 6)

What: We are creating the remote server in AWS

How: Create a free account in amazon console and login to create an EC2 instance

Why: To show how we are going to mount the directory from Ubuntu using SSHFS, we need a remote server.

2) .pem file will be obtained at the end of your instance.

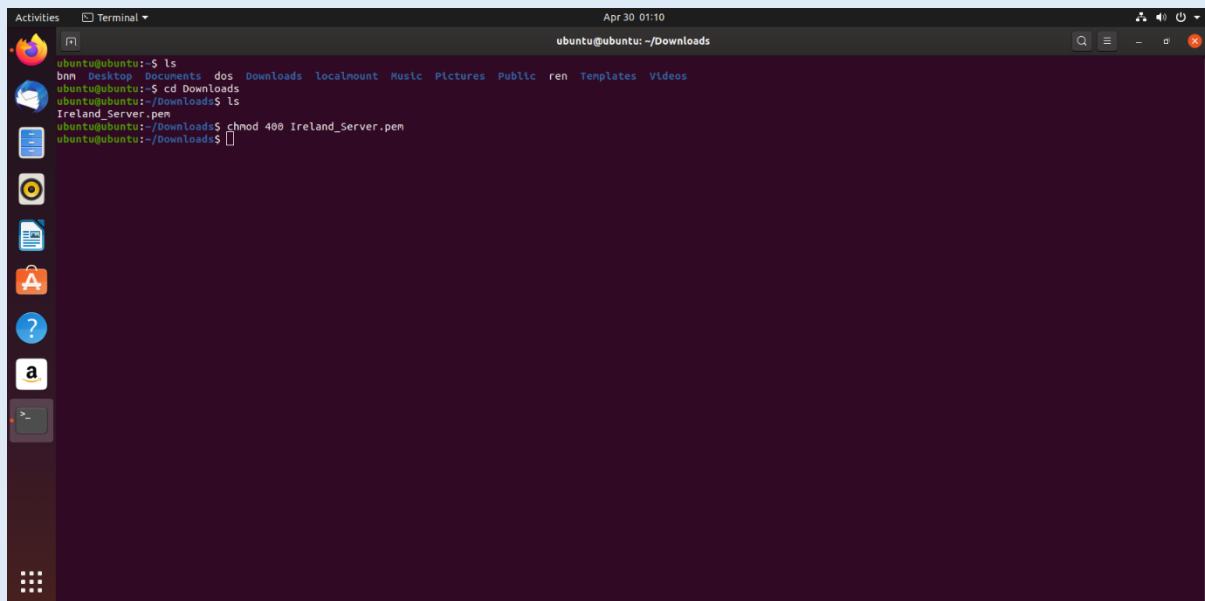
.pem definition: A file with the PEM file extension is a Privacy Enhanced Mail Certificate file used to privately transmit email. The person receiving this email can be confident that the message wasn't altered during its transmission, wasn't shown to anyone else, and was sent by the person who claims to have sent it. The PEM format arose out of the complication of sending binary data through email. The PEM format encodes binary with base64 so that it exists as an ASCII string. The PEM format has been replaced by newer and more secure technologies but the PEM container is still used today to hold certificate authority files, public and private keys, root certificates, etc.

What: .pem file has got public and private keys to access the remote server. Here, we created a server in Ireland and downloaded it's .pem file.

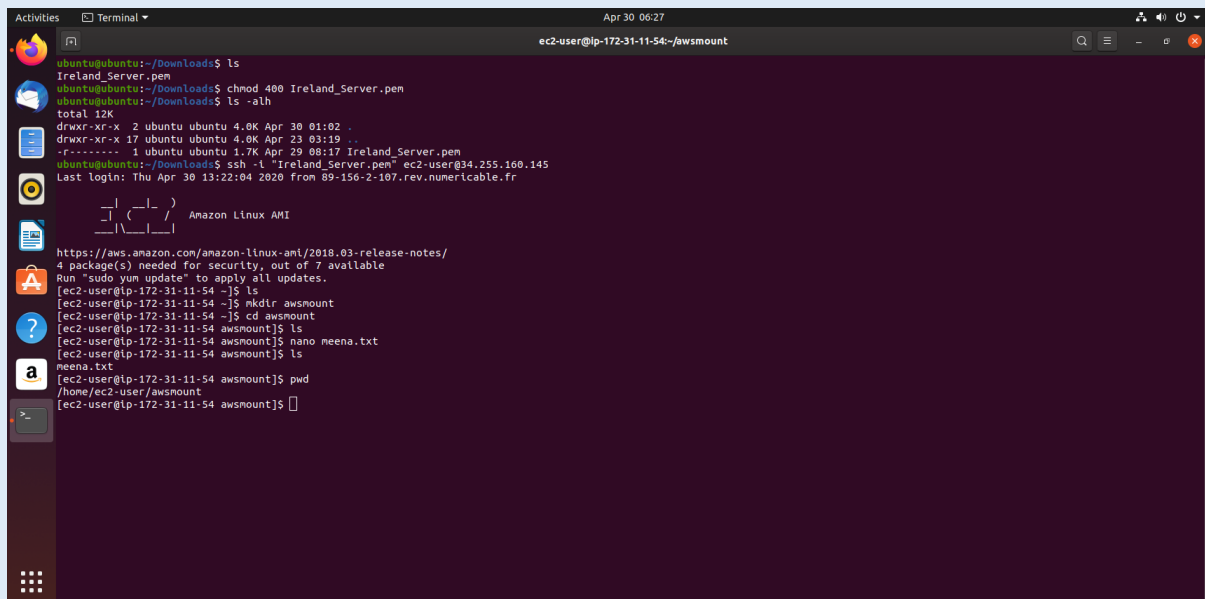
How: After creating the instance, (.pem) will be downloaded

Why: To access or mount the directory in the remote server we need .pem file.

- 3) Check for the .pem file getting downloaded at the end.
- 4) Go to ubuntu and check in downloads with the command “**cd Downloads**”



```
ubuntu@ubuntu:~$ ls
bin  Desktop  documents  dos  Downloads  localmount  Music  Pictures  Public  ren  Templates  Videos
ubuntu@ubuntu:~$ cd Downloads
ubuntu@ubuntu:~/Downloads$ ls
Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ chmod 400 Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$
```



```
ubuntu@ubuntu:~/Downloads$ ls
Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ chmod 400 Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ ls -alh
total 12K
drwxr-xr-x  2 ubuntu ubuntu 4.0K Apr 30 01:02 .
drwxr-xr-x 17 ubuntu ubuntu 4.0K Apr 23 03:19 ..
-r-----  1 ubuntu ubuntu 1.7K Apr 29 08:17 Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ ssh -t "Ireland_Server.pem" ec2-user@34.255.160.145
Last login: Thu Apr 30 13:22:04 2020 From 89-156-2-107.rev.numericable.fr

 _ _ _ _ _
| | ( _ | _ )
|_| \_|_|_|

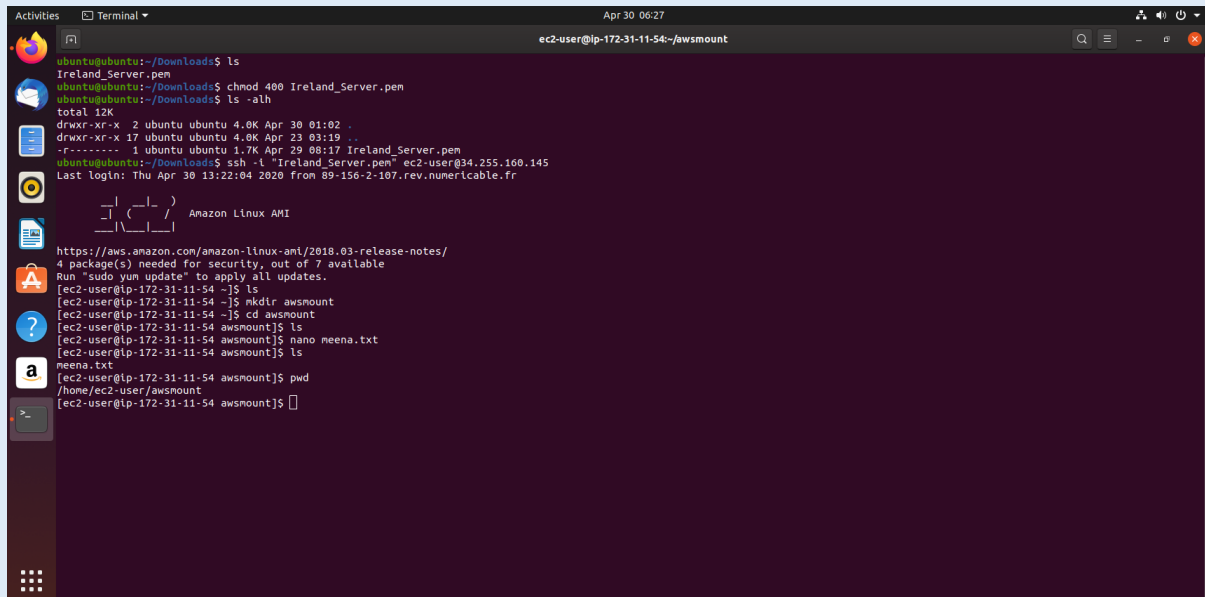
Amazon Linux AMI

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
4 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-11-54 ~]$ ls
[ec2-user@ip-172-31-11-54 ~]$ mkdir awsmount
[ec2-user@ip-172-31-11-54 ~]$ cd awsmount
[ec2-user@ip-172-31-11-54 awsmount]$ ls
[ec2-user@ip-172-31-11-54 awsmount]$ nano meena.txt
[ec2-user@ip-172-31-11-54 awsmount]$ ls
meena.txt
[ec2-user@ip-172-31-11-54 awsmount]$ pwd
/home/ec2-user/awsmount
[ec2-user@ip-172-31-11-54 awsmount]$
```

- 5) Make the file readable by giving the below command
“**Chmod 400 Ireland_Server.pem**”
- 6) Connect to the Ireland server with the help of the EC2's username and server's public address
“**ssh -i “Ireland_Server.pem” ec2-user@34.255.160.145**”
- 7) The responses for the above command would be like
Do you want to continue fingerprinting? then give yes

For the first time you would get the warning stating: Permanently added “remote server’s public address” to the list of known hosts and it would say “welcome to the ubuntu remote sever”

If not first time, it will give the last login date into that server



```
ubuntu@ubuntu:~/Downloads$ ls
Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ chmod 400 Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ ls -alh
total 12K
drwxr-xr-x  2 ubuntu ubuntu 4.0K Apr 30 01:02 .
drwxr-xr-x 17 ubuntu ubuntu 4.0K Apr 23 03:19 ..
-r-----  1 ubuntu ubuntu 1.7K Apr 29 08:17 Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ ssh -t "Ireland_Server.pem" ec2-user@34.255.160.145
Last login: Thu Apr 30 13:22:04 2020 from 89-156-2-107.rev.numericable.fr

      _ _ _
     /   /
    /___/
   /___/
  /___/
 /___/
/___/

Amazon Linux AMI

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
4 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-11-54 ~]$ ls
[ec2-user@ip-172-31-11-54 ~]$ mkdir awsmount
[ec2-user@ip-172-31-11-54 ~]$ cd awsmount
[ec2-user@ip-172-31-11-54 awsmount]$ ls
[ec2-user@ip-172-31-11-54 awsmount]$ nano meena.txt
meena.txt
[ec2-user@ip-172-31-11-54 awsmount]$ pwd
/home/ec2-user/awsmount
[ec2-user@ip-172-31-11-54 awsmount]$
```

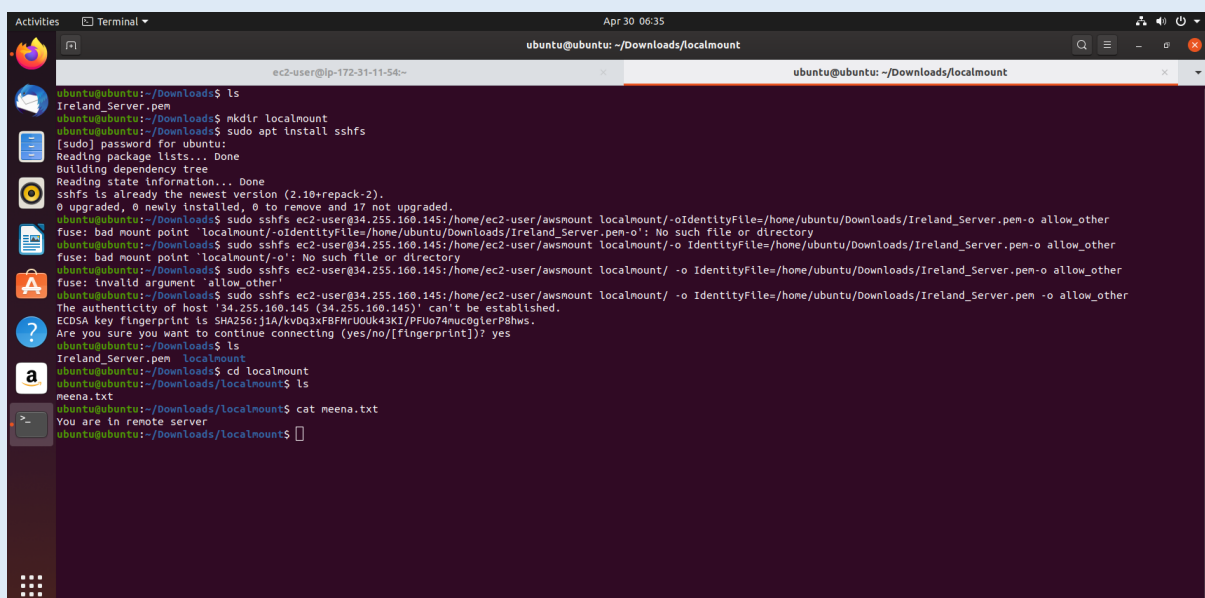
8) We are in the remote server now. Give the command **ls** and check. Then create a directory like “**mkdir awsmount**”

awsmount -name of the directory which is created in remote server

9) “**cd awsmount**” will direct you into that directory

10) Create a file using the command: “**nano meena.txt**”

11) Get the path of that file by giving “**pwd**”



```
ubuntu@ubuntu:~/Downloads$ ls
Ireland_Server.pem
ubuntu@ubuntu:~/Downloads$ mkdir localmount
ubuntu@ubuntu:~/Downloads$ sudo apt install sshfs
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
sshfs is already the newest version (2.10+repack-2).
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
ubuntu@ubuntu:~/Downloads$ sudo sshfs ec2-user@34.255.160.145:/home/ec2-user/awsmount localmount/-o IdentityFile=/home/ubuntu/Downloads/Ireland_Server.pem-o allow_other
fuse: bad mount point 'localmount/-o IdentityFile=/home/ubuntu/Downloads/Ireland_Server.pem-o': No such file or directory
ubuntu@ubuntu:~/Downloads$ sudo sshfs ec2-user@34.255.160.145:/home/ec2-user/awsmount localmount/-o IdentityFile=/home/ubuntu/Downloads/Ireland_Server.pem-o allow_other
fuse: bad mount point 'localmount/-o': No such file or directory
ubuntu@ubuntu:~/Downloads$ sudo sshfs ec2-user@34.255.160.145:/home/ec2-user/awsmount localmount/ -o IdentityFile=/home/ubuntu/Downloads/Ireland_Server.pem-o allow_other
fuse: invalid argument 'allow_other'
ubuntu@ubuntu:~/Downloads$ sudo sshfs ec2-user@34.255.160.145:/home/ec2-user/awsmount localmount/ -o IdentityFile=/home/ubuntu/Downloads/Ireland_Server.pem -o allow_other
The authenticity of host '34.255.160.145 (34.255.160.145)' can't be established.
ECDSA key fingerprint is SHA256:jj1A/kvDq3xFBFmU0Uk43K1/PFU074mucGlerP8hws.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
ubuntu@ubuntu:~/Downloads$ ls
Ireland_Server.pem localmount
ubuntu@ubuntu:~/Downloads$ cd localmount
ubuntu@ubuntu:~/Downloads/localmount$ ls
meena.txt
ubuntu@ubuntu:~/Downloads/localmount$ cat meena.txt
You are in remote server
ubuntu@ubuntu:~/Downloads/localmount$
```

12) Now go to another terminal and check you are in local ubuntu machine

Giving “ls” you will see the .pem file in your local machine as you have downloaded already

13) Create a directory “**mkdir localmount**” in your machine

14) Then we try to install sshfs by giving “**sudo apt install sshfs**”

15) **sudo sshfs {username}@{ipaddress}:{remote folder path} {local folder path} -o IdentityFile={full path to the private key file} -o allow_other**

The above command is used to link the remote folder in the local folder with which we can access the file and edit the file created in remote server

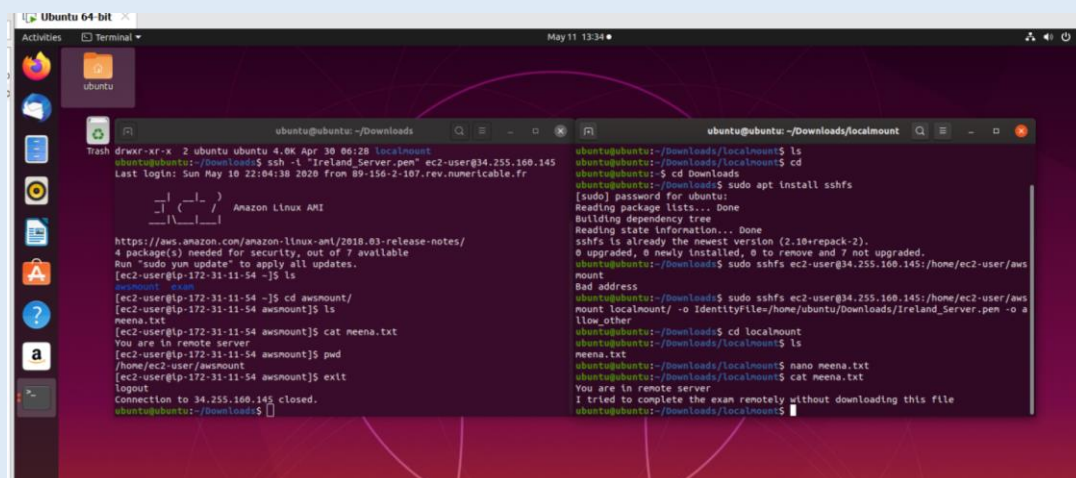
(sudo is a program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user, by default the superuser. It originally stood for "superuser do" as the older versions of sudo were designed to run commands only as the superuser)

16) Give “yes” to continue connecting

17) Give “ls” and then go into the localmount directory created giving “**cd localmount**”

18) When you give ls, you will see the file which was created in the remote server would be present here. This indicates your command in step 15 executed successfully.

19) Now you can edit the file in the remote directory from the local machine without downloading the file



20) Give “**exit**” and close the connection with the remote server after completing your mounting/editing.

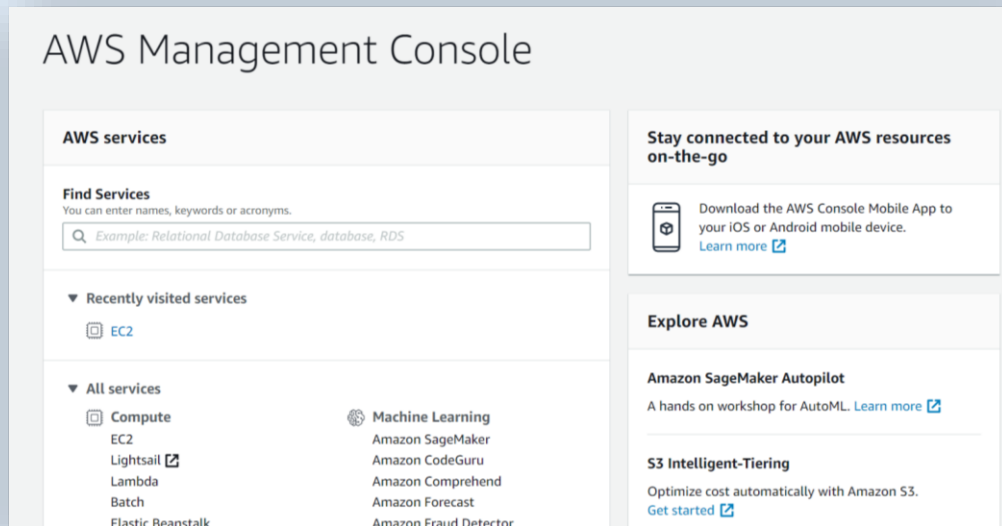
Acronyms used:

EC2	Elastic Compute Cloud
. pem	privacy enhanced mail
ECDSA	Elliptic Curve Digital Signature Algorithm
ssh -i	Secure Socket Shell Identity File
mkdir	Make directory
chmod	Change mode

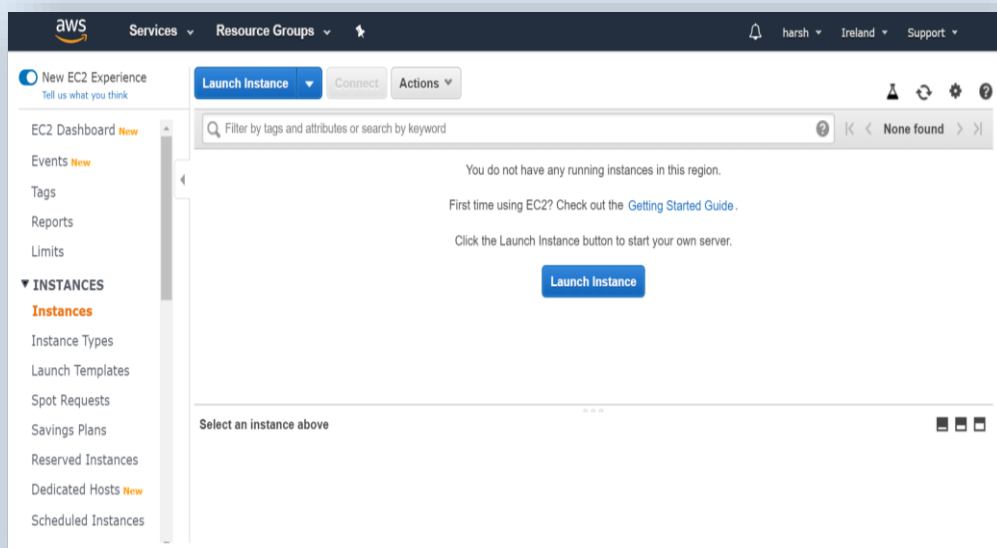
AWS EC2 Instance (Remote server) creation screenshots:

NOTE: we are creating the test server here in remote region by opening the free account in <https://aws.amazon.com/>

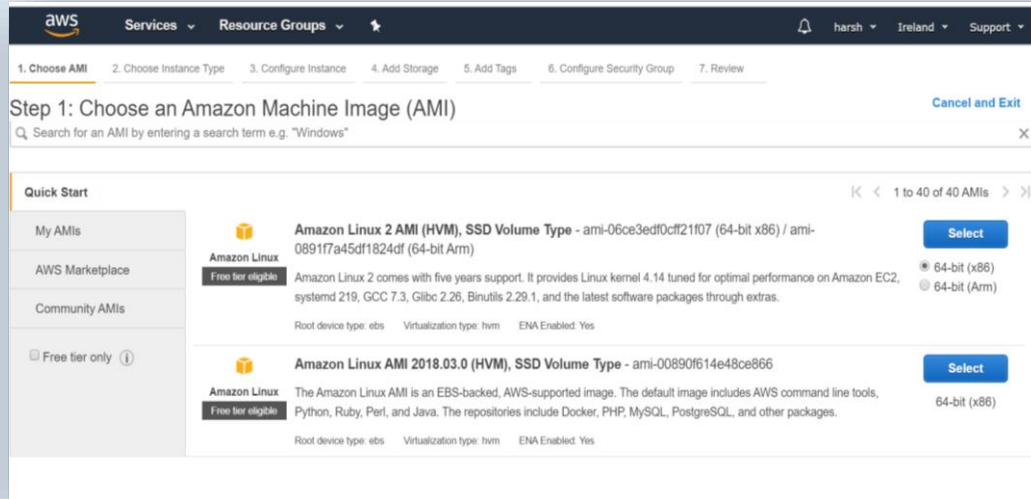
1) When you login search for EC2 services



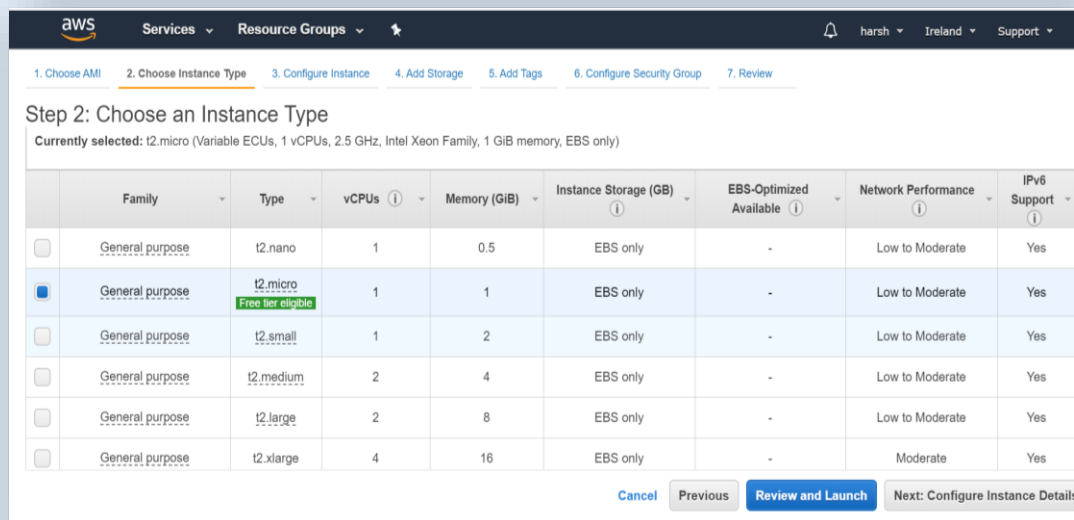
2) In the top right, select the region where you want to create the server. Here I chose "Ireland" and you could see that there is no instance running in that region.



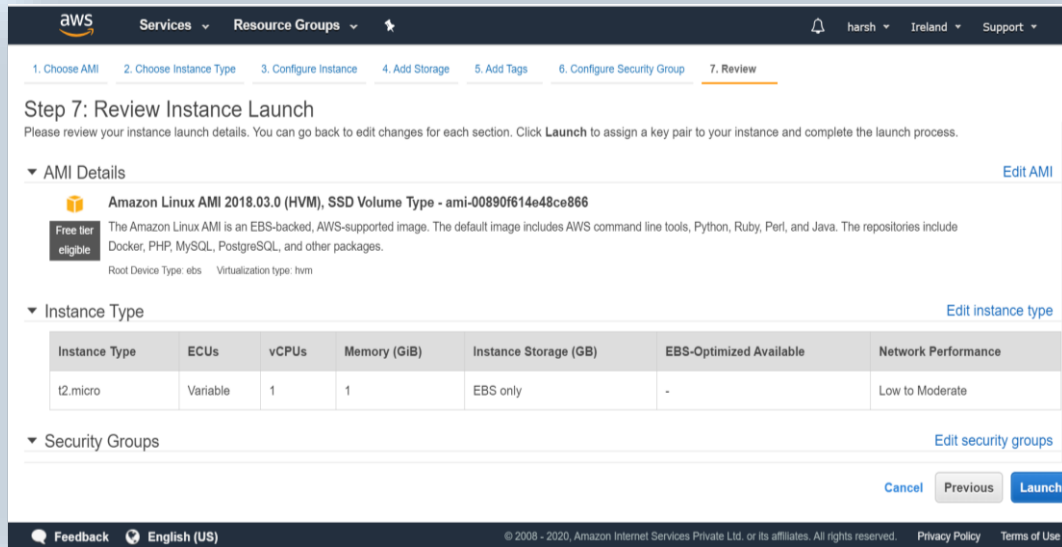
3) Choose the AMI according to your operating system



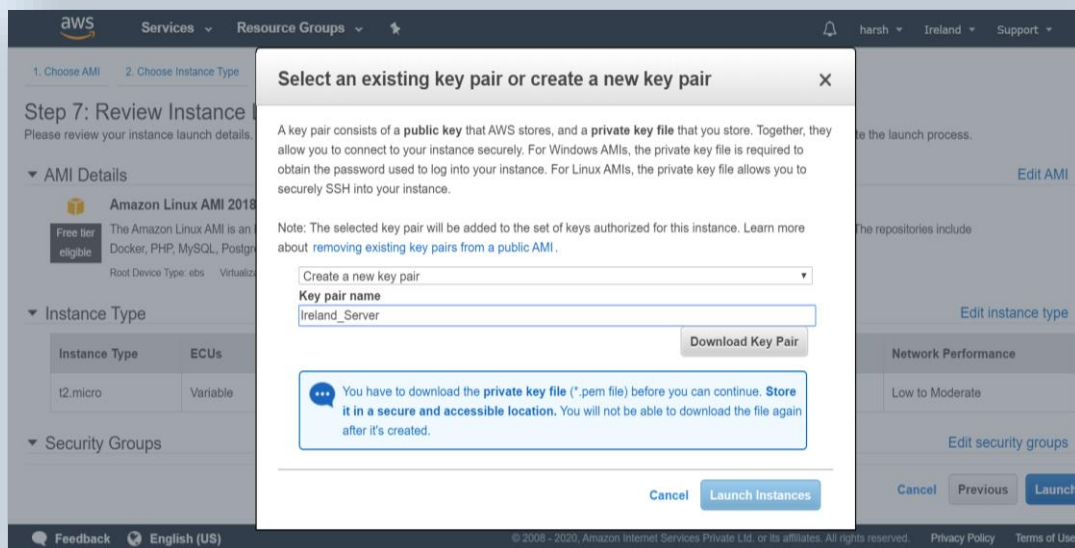
4) Choose the free version for the type of instance here



5) In the 6 Configure Security Group, choose the default security group and in “Inbound rules” allow all traffic for “My IP”. Then click on to 7 Review and then launch.

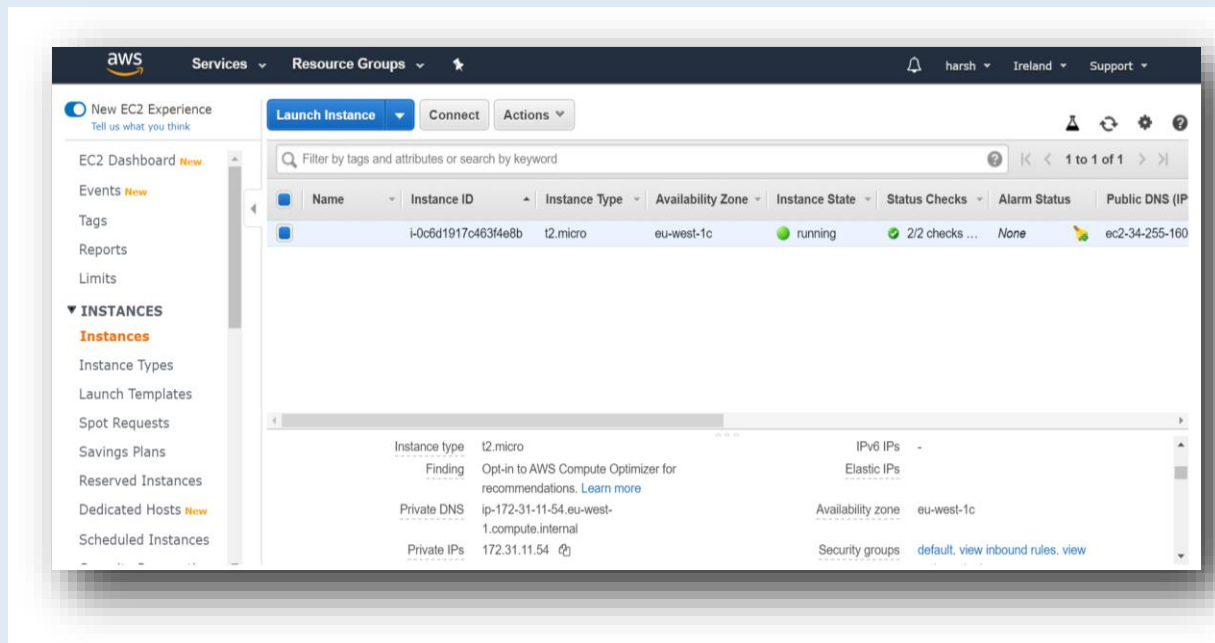


6) In the final step create a new key pair in which .pem file is downloaded



Hence ".pem file" is downloaded

7) You can see the instance is running in Ireland. You can see the public DNS address. Note down the public DNS address to communicate to the remote server.



Video link:

<https://youtu.be/RxmdcL8CVtw>

Reference: <https://stackoverflow.com/questions/22217767/how-to-mount-a-folder-on-amazon-ec2-instance-with-private-key-using-sshfs>

THANK YOU