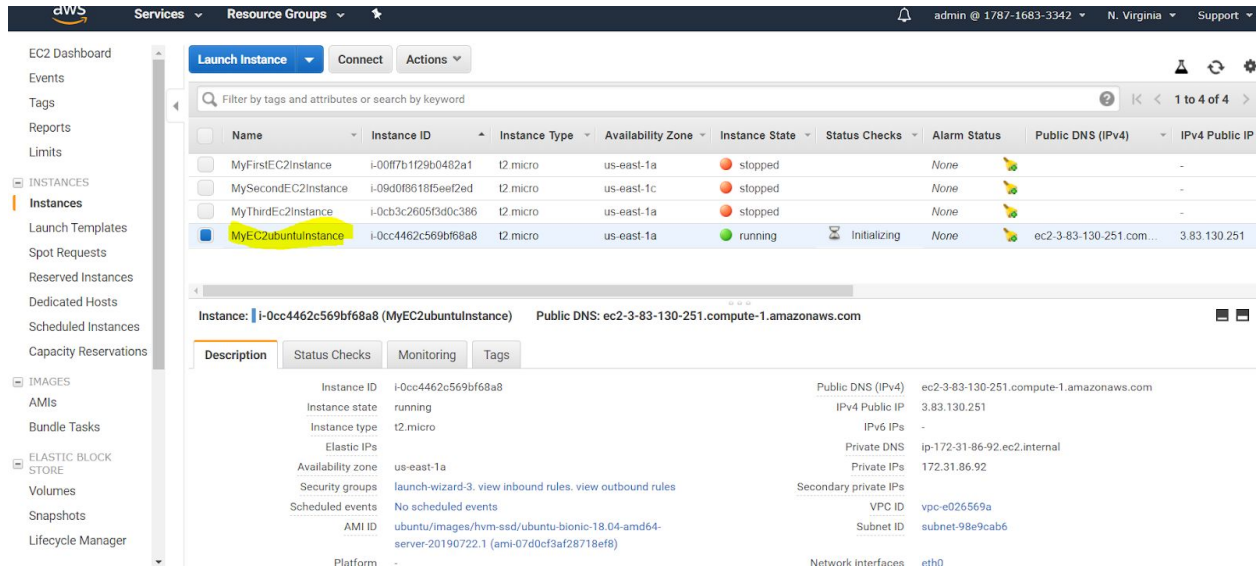


AWS EC2 launch ubuntu machine

Exercise: Access ubuntu from Windows

1) Create a new Ubuntu Instance



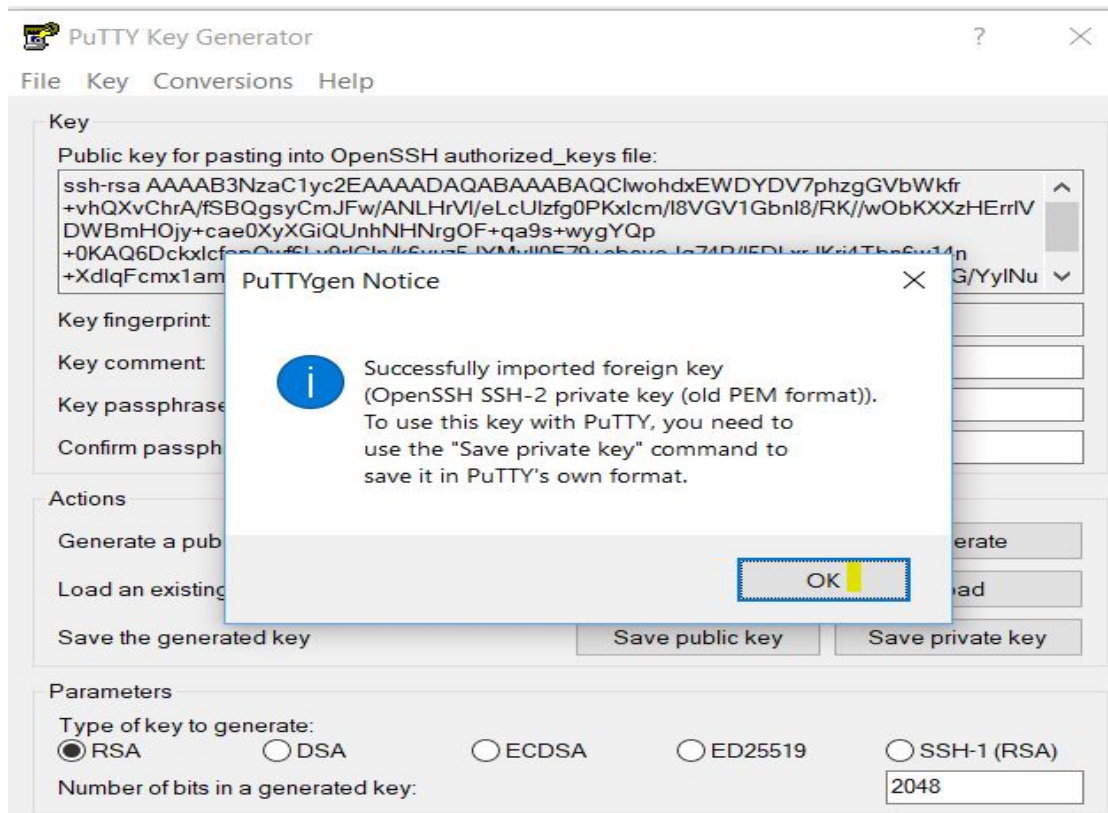
The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'EC2 Dashboard', 'Events', 'Tags', 'Reports', 'Limits', 'INSTANCES', 'Launch Templates', 'Spot Requests', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', 'IMAGES', 'AMIs', 'Bundle Tasks', 'ELASTIC BLOCK STORE', 'Volumes', 'Snapshots', and 'Lifecycle Manager'. The 'INSTANCES' section is selected. The main panel displays a table of EC2 instances. The instance 'MyEC2ubuntuInstance' is highlighted. Below the table, the details for this instance are shown, including its ID, state, type, availability zone, security groups, and public IP address.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
MyFirstEC2Instance	i-00ff7b129b0482a1	t2.micro	us-east-1a	stopped	None	None	-	-
MySecondEC2Instance	i-09d0f8618f5ae2ed	t2.micro	us-east-1c	stopped	None	None	-	-
MyThirdEC2Instance	i-0cb3c2605f3d0c386	t2.micro	us-east-1a	stopped	None	None	-	-
MyEC2ubuntuInstance	i-0cc4462c569bf68a8	t2.micro	us-east-1a	running	Initializing	None	ec2-3-83-130-251.com...	3.83.130.251

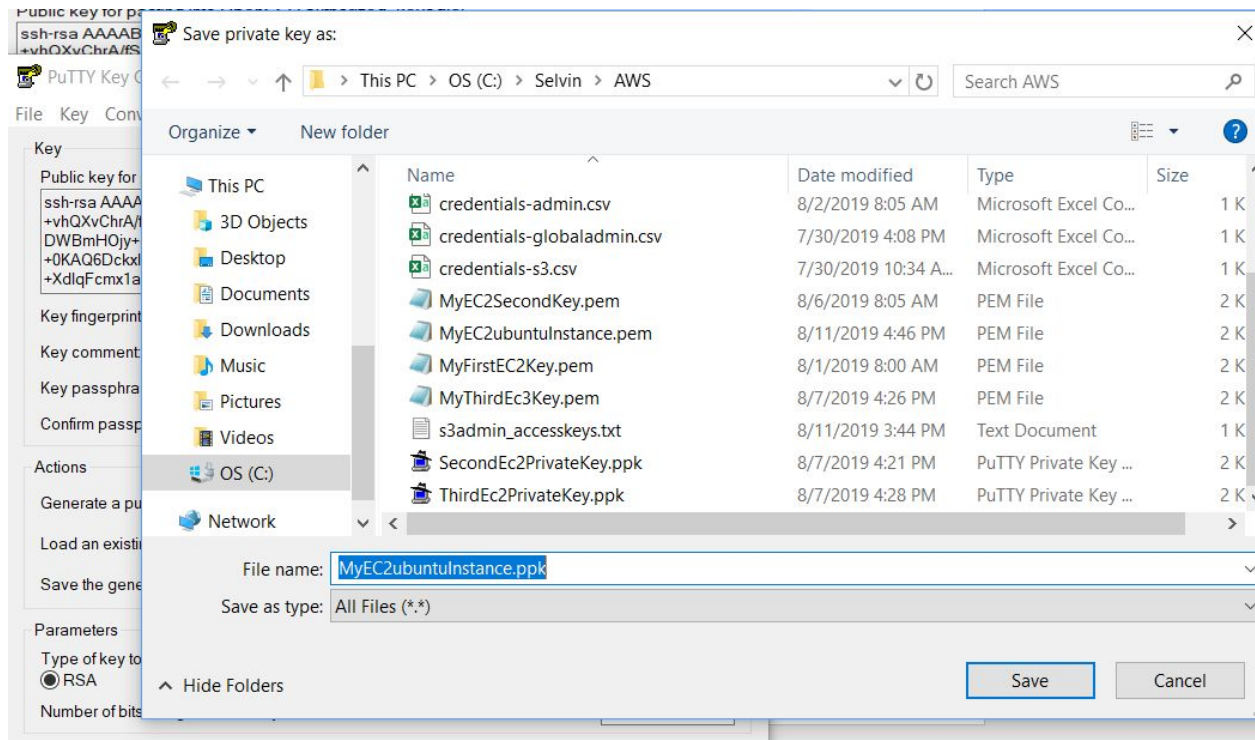
Instance: **i-0cc4462c569bf68a8 (MyEC2ubuntuInstance)** Public DNS: **ec2-3-83-130-251.compute-1.amazonaws.com**

Description	Status Checks	Monitoring	Tags
Instance ID	i-0cc4462c569bf68a8		
Instance state	running		
Instance type	t2.micro		
Elastic IPs			
Availability zone	us-east-1a		
Security groups	launch-wizard-3, view inbound rules, view outbound rules		
Scheduled events	No scheduled events		
AMI ID	ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20190722.1 (ami-07d0cf3af28718ef8)		
Platform	-		
Public DNS (IPv4)	ec2-3-83-130-251.compute-1.amazonaws.com		
IPv4 Public IP	3.83.130.251		
IPv6 IPs	-		
Private DNS	ip-172-31-86-92.ec2.internal		
Private IPs	172.31.86.92		
Secondary private IPs			
VPC ID	vpc-e026569a		
Subnet ID	subnet-98e9cab6		
Network interfaces	eth0		

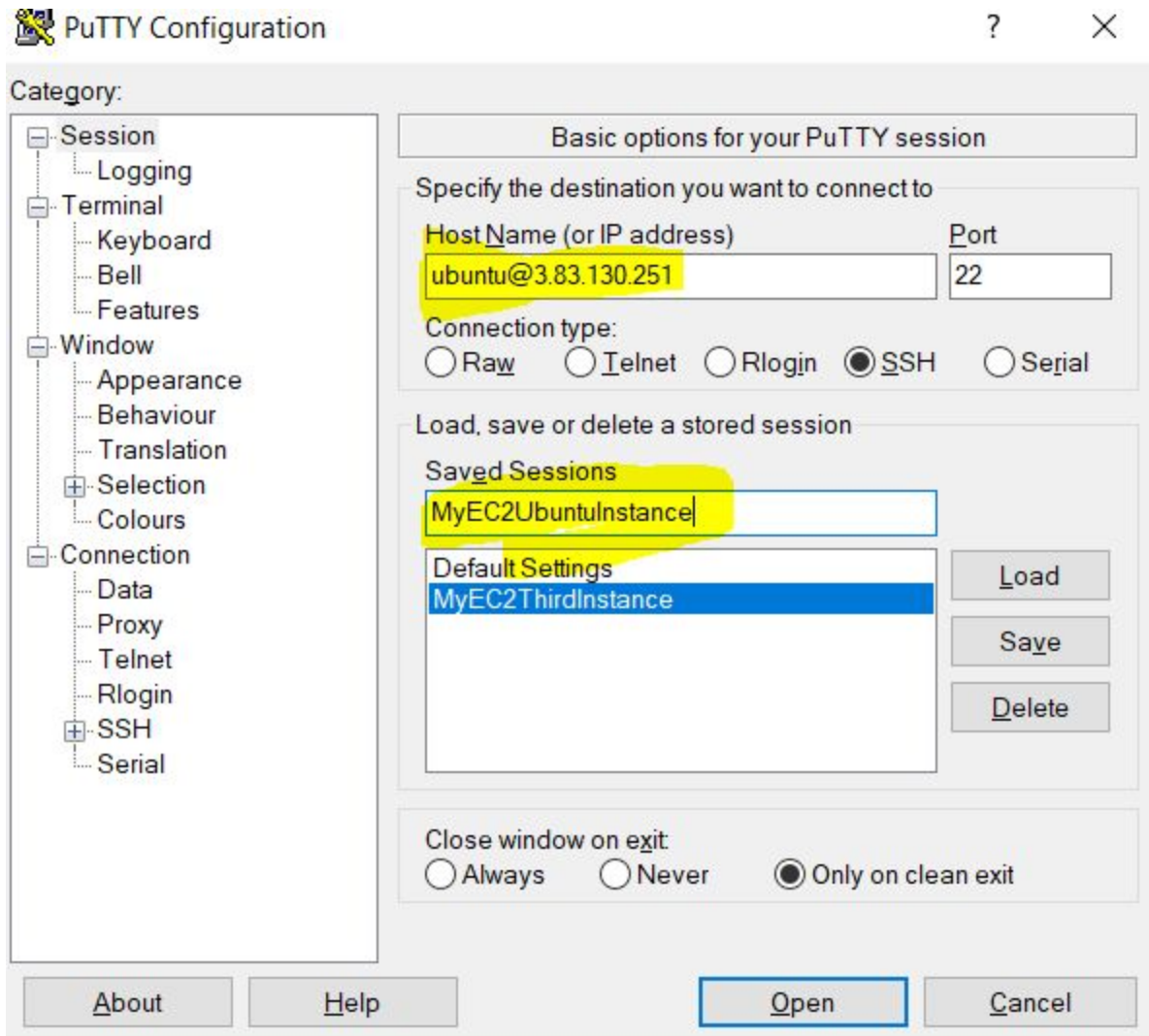
2) Using Puttygen, convert the .pem file to private key.



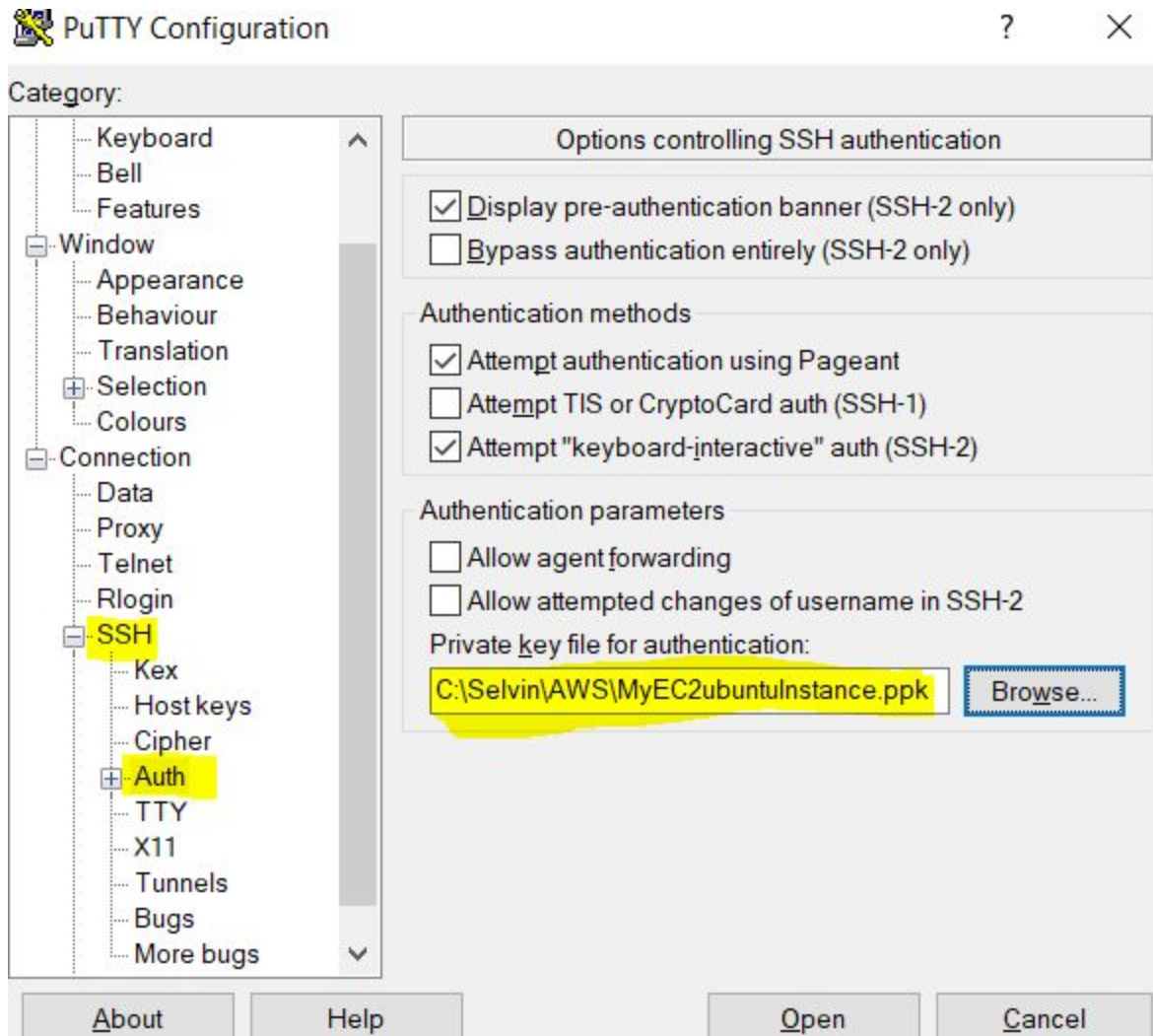
3) Click "Save Private Key" to save the private key.



4) Open Putty and save session
HostName: ubuntu@ipaddress



5) Load the Private Key
Expand SSH and click "Auth"



6) By Clicking open, ubuntu instance will be opened

```
ubuntu@ip-172-31-86-92: ~  
Using username "ubuntu".  
Authenticating with public key "imported-openssh-key"  
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-1044-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sun Aug 11 11:30:28 UTC 2019  
  
System load:  0.0                Processes:            85  
Usage of /:   13.6% of 7.69GB    Users logged in:     0  
Memory usage: 14%               IP address for eth0: 172.31.86.92  
Swap usage:   0%  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-86-92:~$
```

7) Tested Below Commands

a) whoami

```
ubuntu@ip-172-31-86-92:~$ whoami  
ubuntu  
ubuntu@ip-172-31-86-92:~$
```

b) command to change the password

sudo passwd ubuntu

```
ubuntu@ip-172-31-86-92:~$ sudo passwd ubuntu
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
ubuntu@ip-172-31-86-92:~$
```

- c) to login with this new password next type, the setting in ssh config file needs to be changed. Below commands are used

command to edit sshd-config file

```
sudo vi /etc/ssh/sshd_config
```

search by typing `/password`

edit the file by `i`

escape from edit mode `escape`

save the file `:wq`


```
#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

Once the file is edited restart the instances

```
sudo systemctl restart sshd
```

```
sudo systemctl status sshd
```

By Selvin