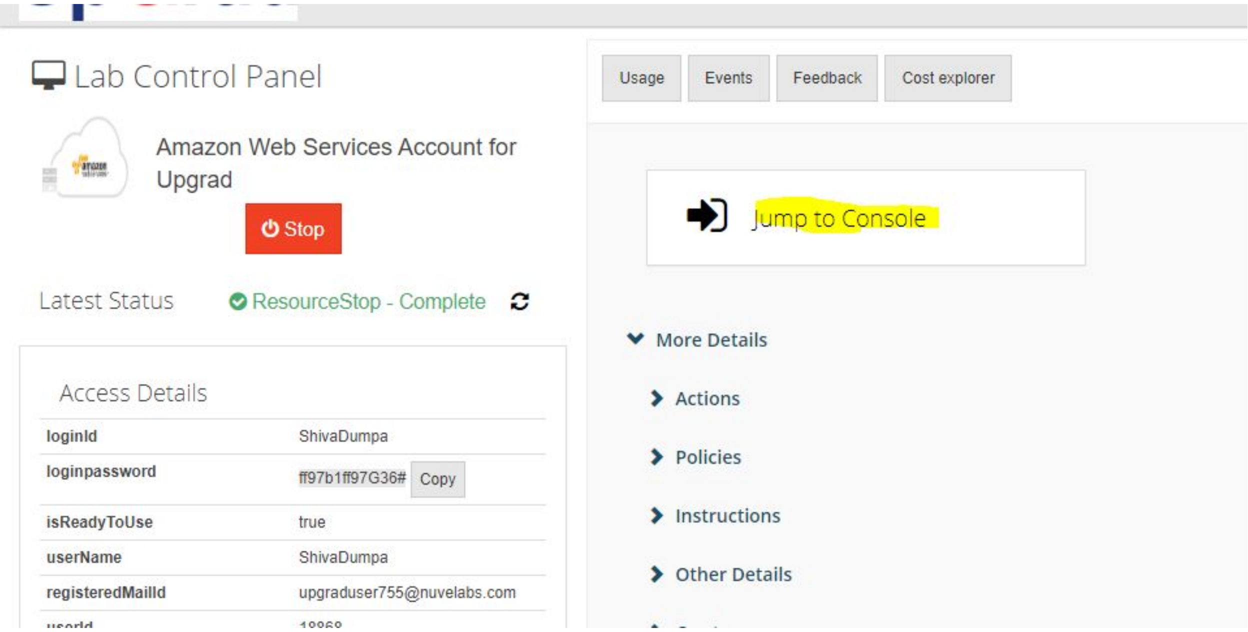
Launching EC2 Instance & Establishing Connection

Launch the EC2 instance on AWS and access Amazon's EC2 server from your local machine using Windows or Linux/Mac OS. Here's the link to AWS EC2:

1. To access the AWS platform, make sure that you have the login credentials. Once you login, you can follow these steps.

   Click to View Lab -> Jump to console tab.

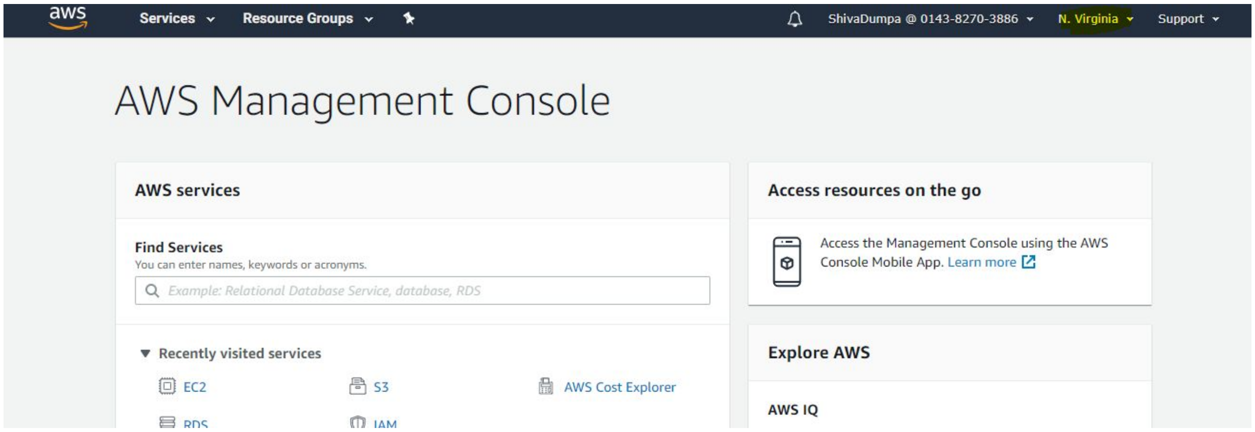


Latest Status ResourceStop - Complete

Access Details

loginId	ShivaDumpa
loginpassword	ff97b1ff97G36# Copy
isReadyToUse	true
userName	ShivaDumpa
registeredMailId	upgraduser755@nuvelabs.com
userId	18868

2. After signing in, select region **N.Virginia**. from the drop-down menu at the top-right corner.



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS

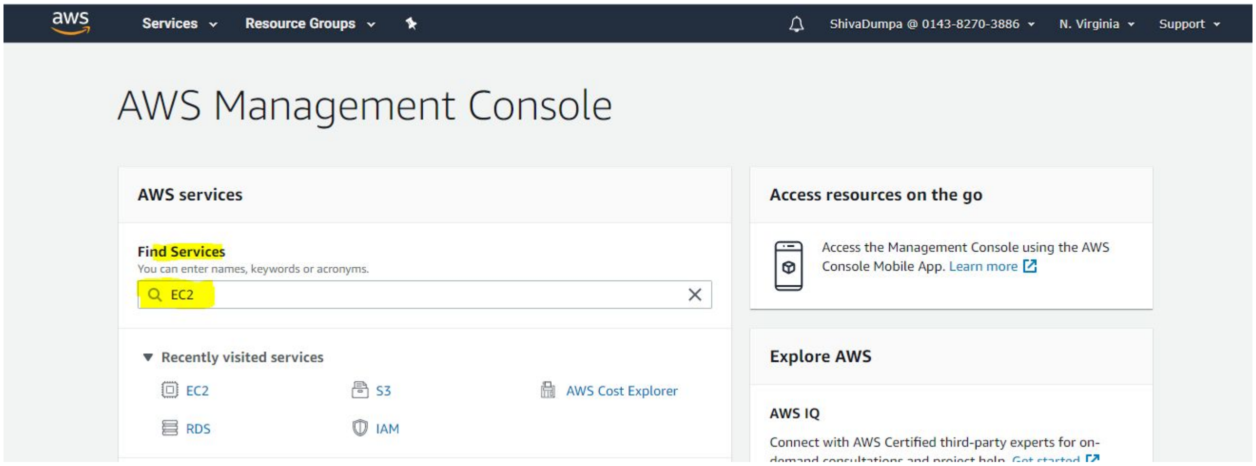
Recently visited services
EC2 S3 AWS Cost Explorer
RDS IAM

Access resources on the go
Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

AWS IQ

3. **Click** on **EC2** that is shown below the ‘Services’ under ‘Find services’.



AWS Management Console

AWS services

Find Services
You can enter names, keywords or acronyms.
EC2

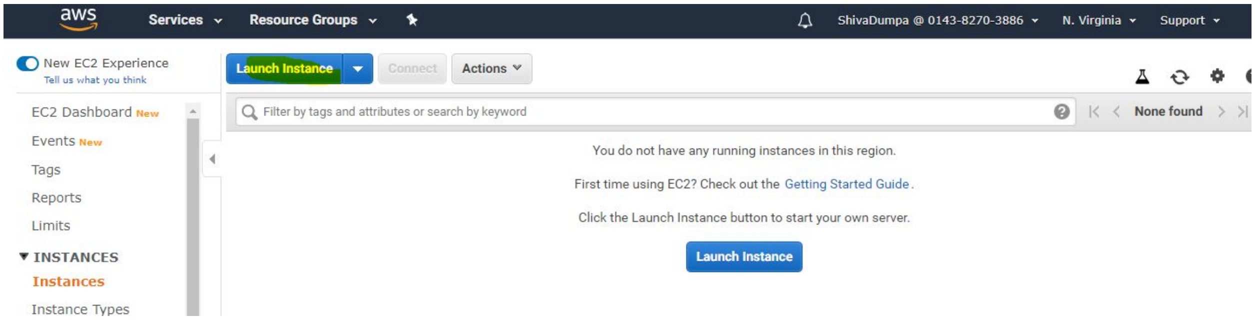
Recently visited services
EC2 S3 AWS Cost Explorer
RDS IAM

Access resources on the go
Access the Management Console using the AWS Console Mobile App. Learn more

Explore AWS

AWS IQ
Connect with AWS Certified third-party experts for on-demand consultations and project help. Get started

4. Then, click on ‘Launch Instance’ as shown below.

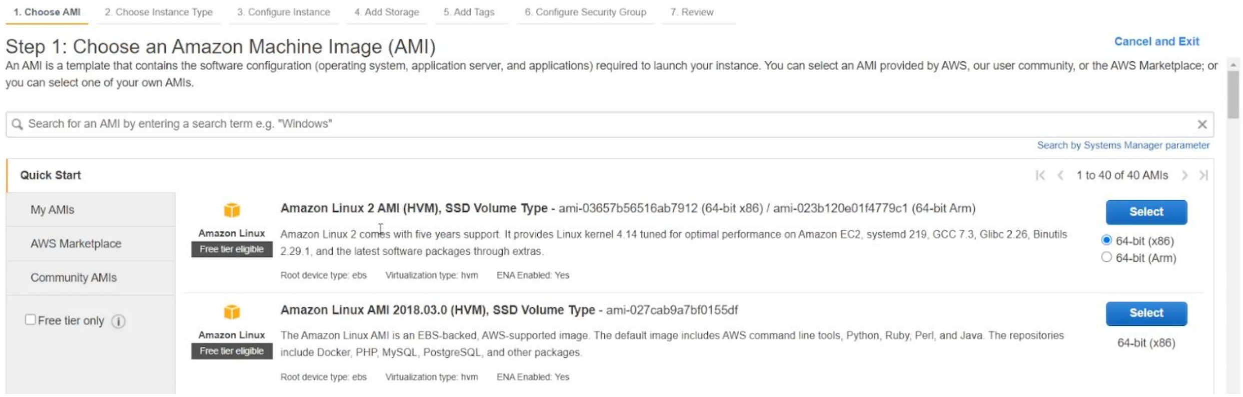


You do not have any running instances in this region.

First time using EC2? Check out the Getting Started Guide.

Click the Launch Instance button to start your own server.

5. In the ‘**Step 1: Choose an Amazon Machine Image’** page, select the **OS** (operating system) you want to install in the instance**.** In this module, we are selecting **“Amazon Linux 2 AMI (HVM), SSD Volume Type”** and **clicking** on Select.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-03657b56516ab7912 (64-bit x86) / ami-023b120e01f4779c1 (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

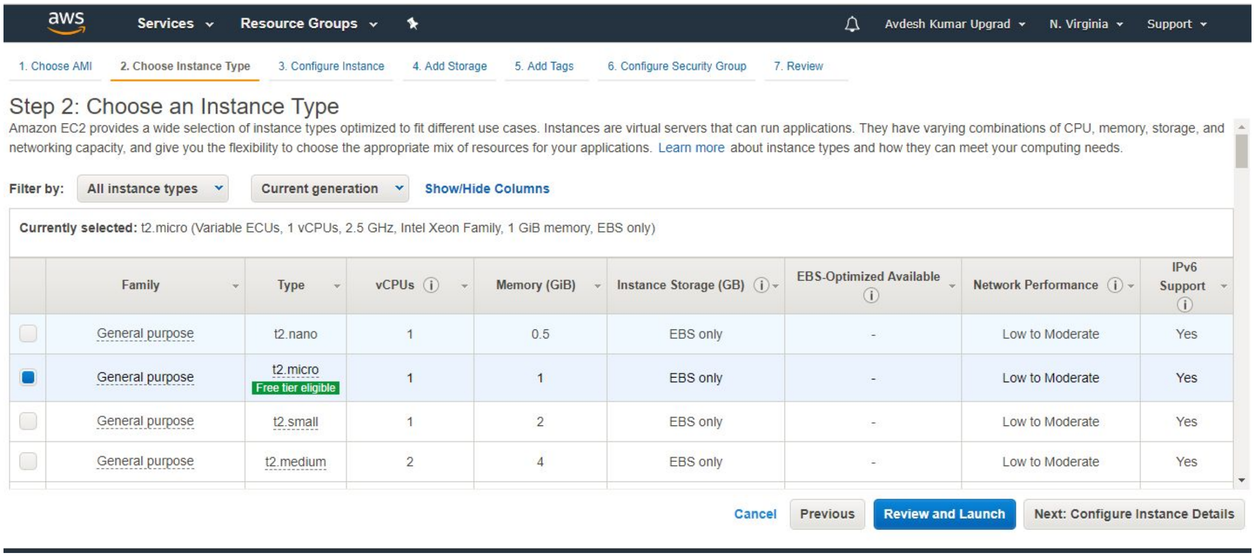
Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-027cab9a7bf0155df

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

6. Next, select the type of machine or the configuration that you need. We recommend you to select a machine with **1 core** (CPUs) and **1 GB memory** — t2.micro .



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

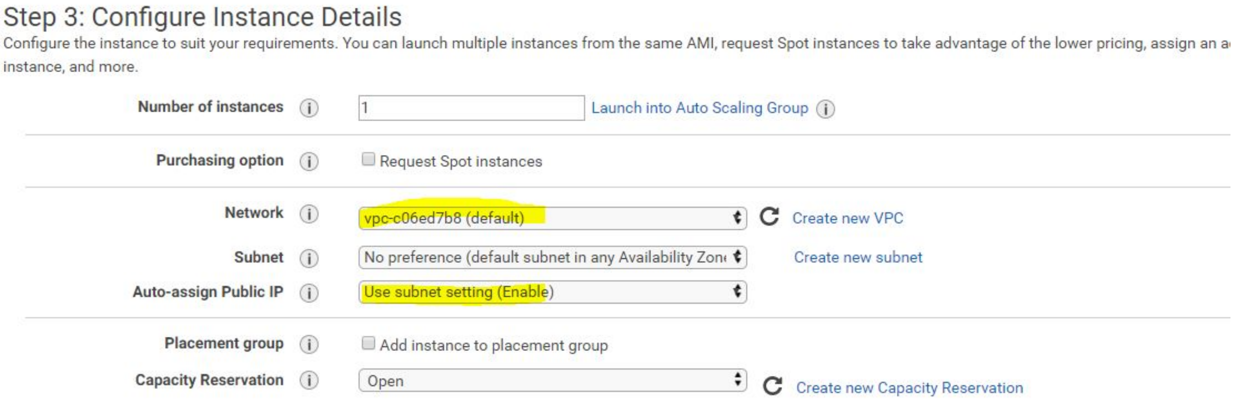
Filter by: All instance types | Current generation | Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

7. Click on 'Next: Configure Instance Details'.
    a. Set the 'Number of instances' to 1.
    b. 'Network' to your VPC name.-default
    c. Auto-assign Public IP- **Enable**

    Keep all other settings unchanged.

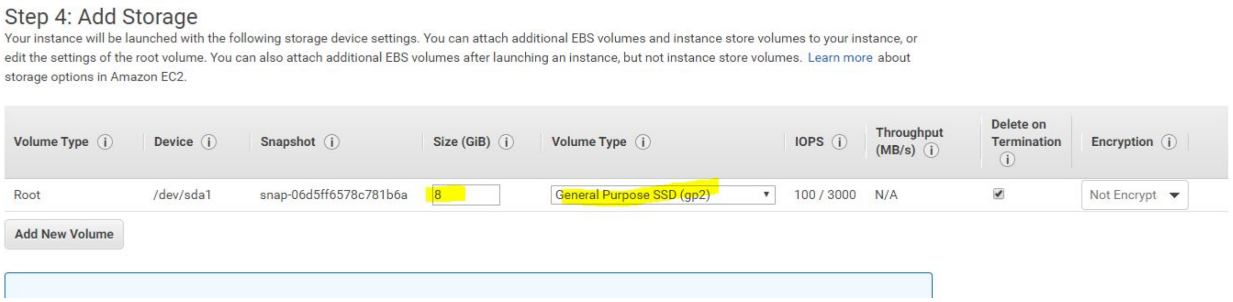

Launch into Auto Scaling Group
Create new VPC
Create new subnet
Create new Capacity Reservation

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an a instance, and more.

Number of instances	1
Purchasing option	□ Request Spot instances
Network	vpc-c06ed7b8 (default)
Subnet	No preference (default subnet in any Availability Zon
Auto-assign Public IP	Use subnet setting (Enable)
Placement group	□ Add instance to placement group
Capacity Reservation	Open

8. Now, click on '**Next: Add Storage**'.

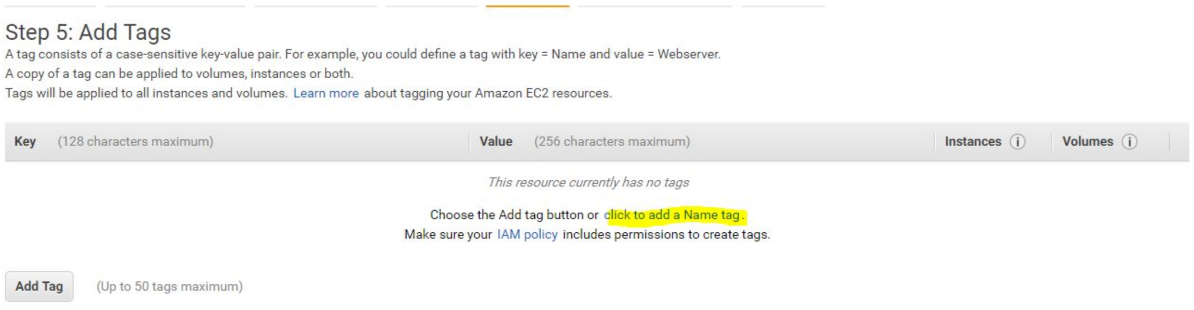


Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/sda1	snap-06d5ff6578c781b6a	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypt

9. Click on '**Next: Add Tags**'. Then Click on '**click to add a Name tag**' as shown in the image below.



Step 5: Add Tags

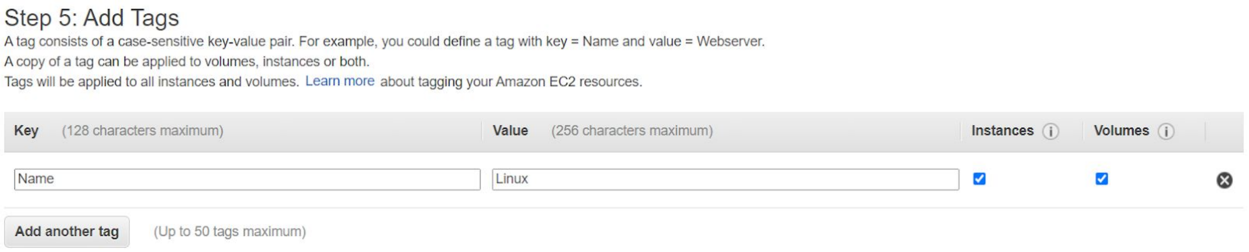
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ

This resource currently has no tags

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

a. Give a name in the cell under **'Value'**. In our case, we have named the instance as 'Linux'.



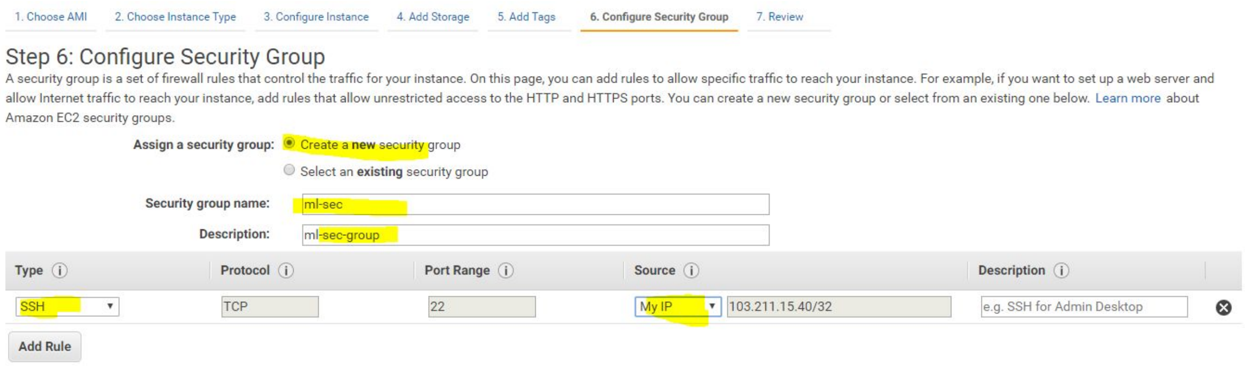
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ
Name	Linux	☑	☑

10. Click on **‘Next: Configure Security Group**’.

    Select the option ‘**Create a new security group**’ and name it as ‘**ml-sec**’. You should select the source as **My IP** for best practice. It automatically puts your system IP address in the section.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: ml-sec

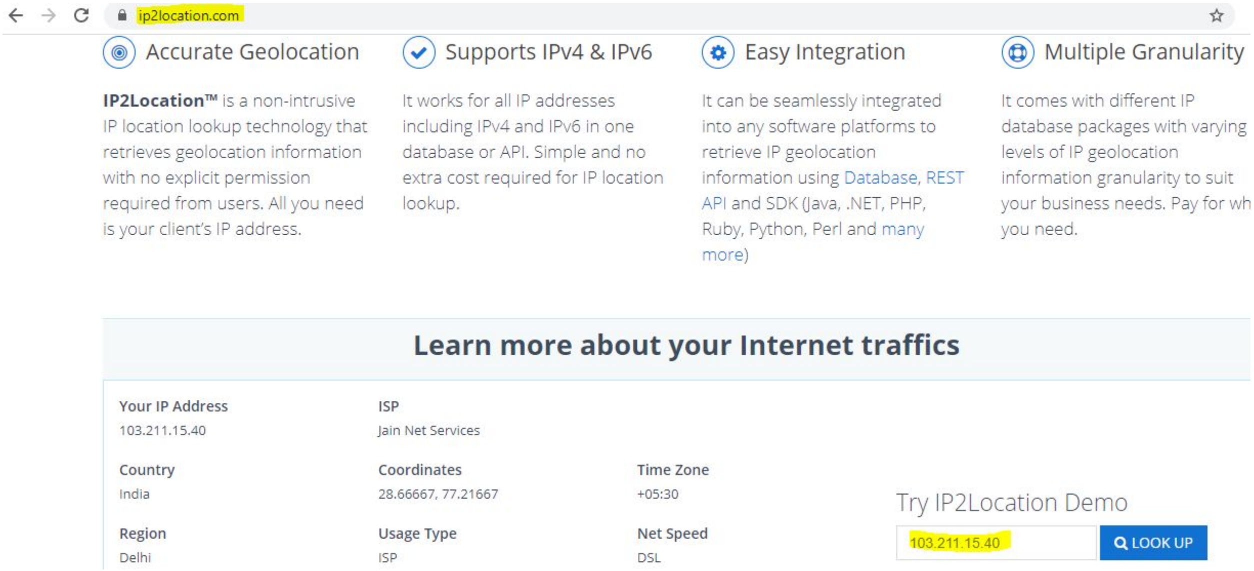
Description: ml-sec-group

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	My IP	103.211.15.40/32	e.g. SSH for Admin Desktop

Note: You can also verify your source ip address or your system ip address using the below link.

https://www.ip2location.com/

You have to be careful when you are using the office laptop or a VPN network. In a few cases, you might not be able to access EC2 instances as your company might have blocked these services. In that case, please use a personal laptop or another network.



Accurate Geolocation

IP2Location™ is a non-intrusive IP location lookup technology that retrieves geolocation information with no explicit permission required from users. All you need is your client's IP address.

Supports IPv4 & IPv6

It works for all IP addresses including IPv4 and IPv6 in one database or API. Simple and no extra cost required for IP location lookup.

Easy Integration

It can be seamlessly integrated into any software platforms to retrieve IP geolocation information using Database, REST API and SDK (Java, .NET, PHP, Ruby, Python, Perl and many more)

Multiple Granularity

It comes with different IP database packages with varying levels of IP geolocation information granularity to suit your business needs. Pay for wh you need.

Learn more about your Internet traffics

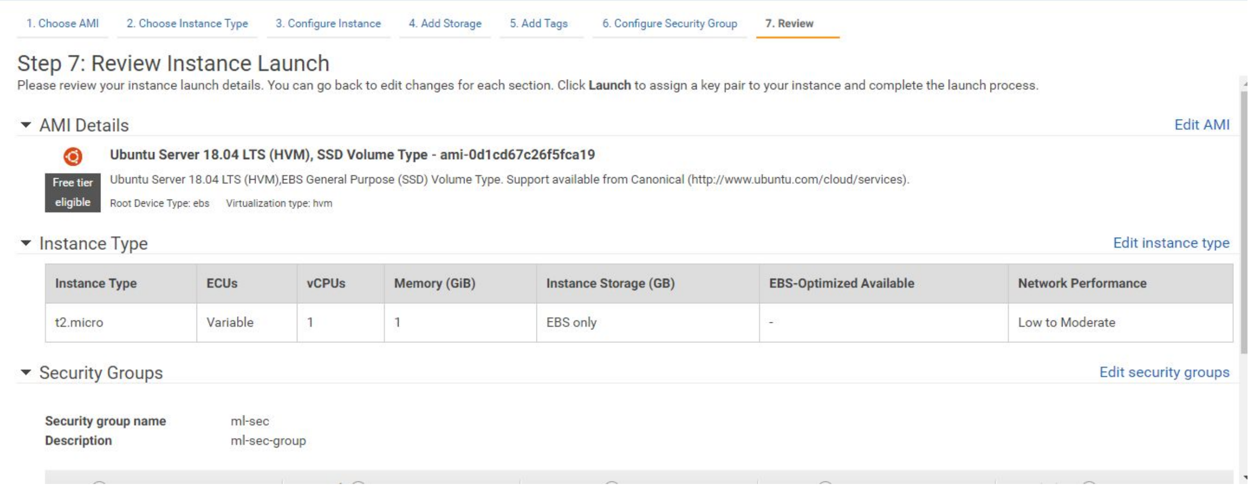
Your IP Address	ISP	
103.211.15.40	Jain Net Services	
Country	**Coordinates**	**Time Zone**
India	28.66667, 77.21667	+05:30
Region	**Usage Type**	**Net Speed**
Delhi	ISP	DSL

Try IP2Location Demo

103.211.15.40 LOOK UP

Then click on “**Review and launch**”

11. Finally, Click on “**Launch**”.



Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details — Edit AMI

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0d1cd67c26f5fca19

Free tier eligible

Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Root Device Type: ebs   Virtualization type: hvm

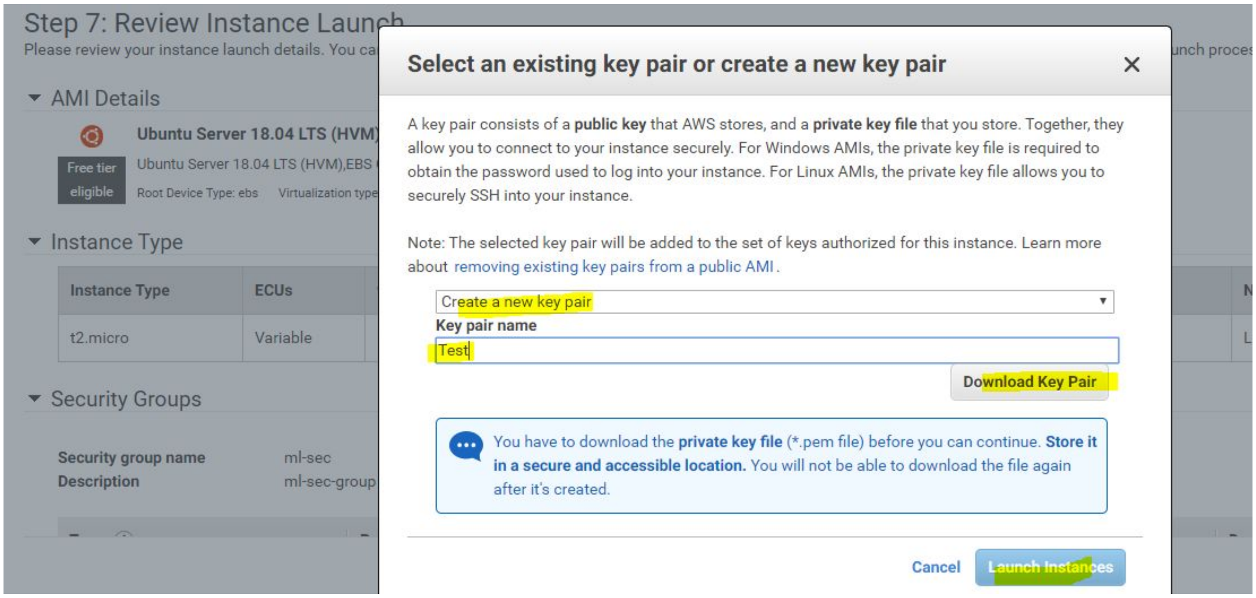
Instance Type — Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups — Edit security groups

Security group name	ml-sec
Description	ml-sec-group

12. After that, select ‘**Create a new key pair**’ give the key pair a name (**Test** in our case), and then click on ‘**Download Key Pair**’.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name

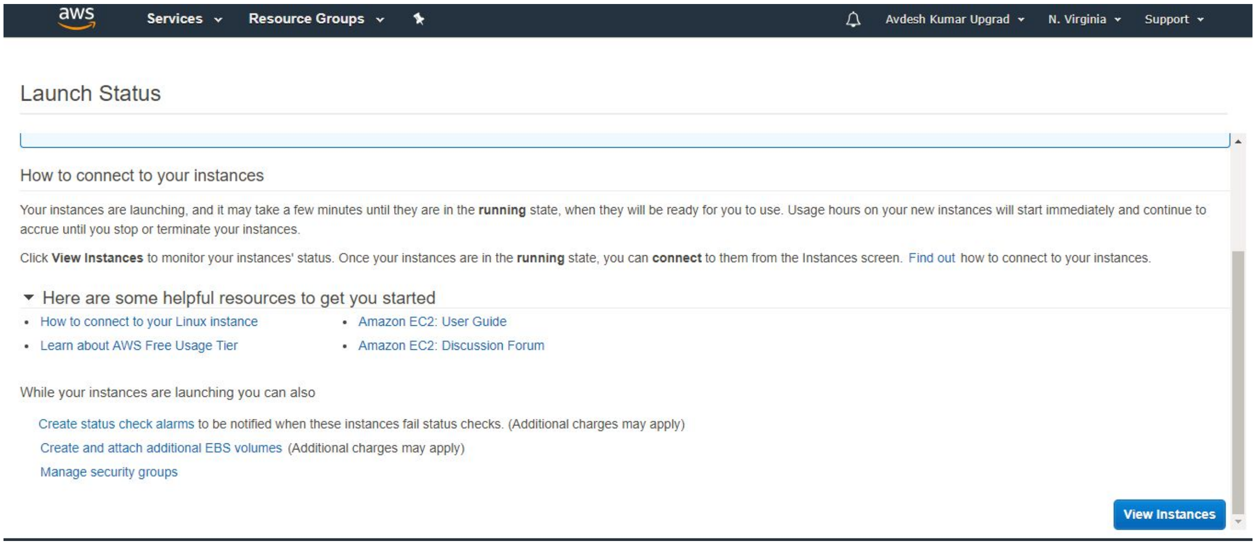
Test

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Note: You must download the pem file as it can’t be accessed again. Also, it gives access to your instance, so please keep it in a safe location and do not share it with anybody.

13. Then, click on ‘**Launch Instances**’.

Your instance is now ready. Click on ‘**View Instances**’ and your instances will appear on the screen, as shown below:



Launch Status

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

Here are some helpful resources to get you started

- How to connect to your Linux instance
- Learn about AWS Free Usage Tier
- Amazon EC2: User Guide
- Amazon EC2: Discussion Forum

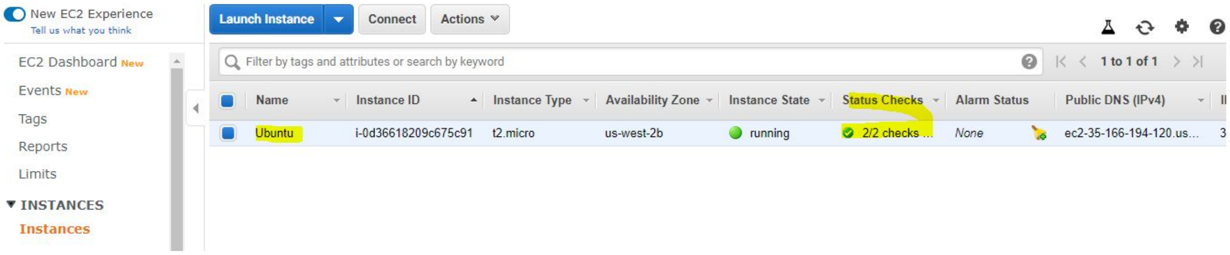
While your instances are launching you can also

Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)

Create and attach additional EBS volumes (Additional charges may apply)

Manage security groups

Check the ‘Status Checks’ column until ‘2/2 checks’ appears.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	I
Ubuntu	i-0d36618209c675c91	t2.micro	us-west-2b	running	2/2 checks ...	None	ec2-35-166-194-120.us...	3

However, there are additional steps to access it from your machine. Let’s try to understand those.

To access the EC2 instance, you must go to the EC2 dashboard. The following steps will be helpful in accessing the ‘EC2’ instance **from a Windows machine**, but you can also use Linux/Mac OS. For Linux/Mac OS, you can follow the steps on page 25 of this document (Titled as “**For Linux/Mac OS users to connect the EC2 Instance.**”)

Connect to the EC2 Instance from a Windows Machine

For Windows users the required software are:

a. PuTTY

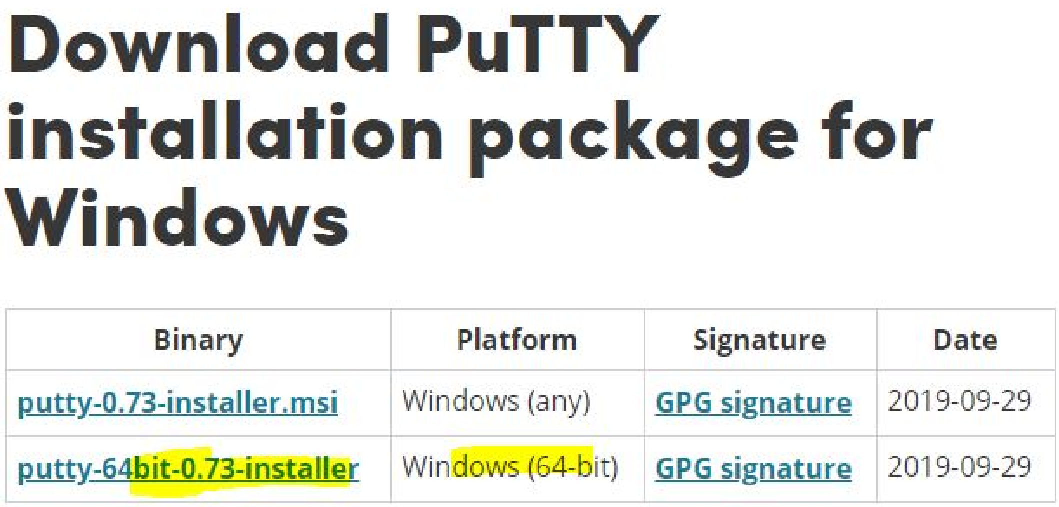
b. PuTTYgen

1. Download and install PuTTY and PuTTYgen from the link below.

https://www.ssh.com/ssh/putty/download#sec-Download-PuTTY-installation-package-for- Windows

Click on the first link:

PuTTY - Secure Download | SSH.COM - SSH Communications Security



Download PuTTY installation package for Windows

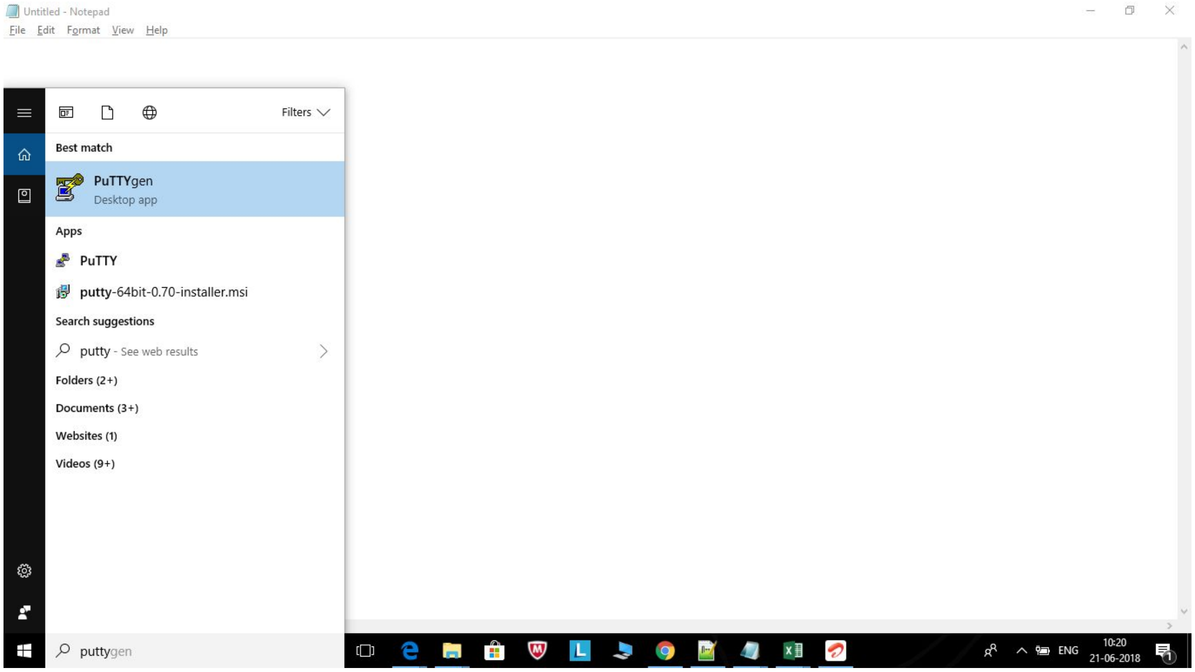
Binary	Platform	Signature	Date
putty-0.73-installer.msi	Windows (any)	GPG signature	2019-09-29
putty-64bit-0.73-installer	Windows (64-bit)	GPG signature	2019-09-29

2. If you have a 32-bit OS, then you need to install putty-0.73-installer.msi. And if you have a 64-bit OS, then choose the latest 64-bit installer file. The file will automatically download after you click on the link.

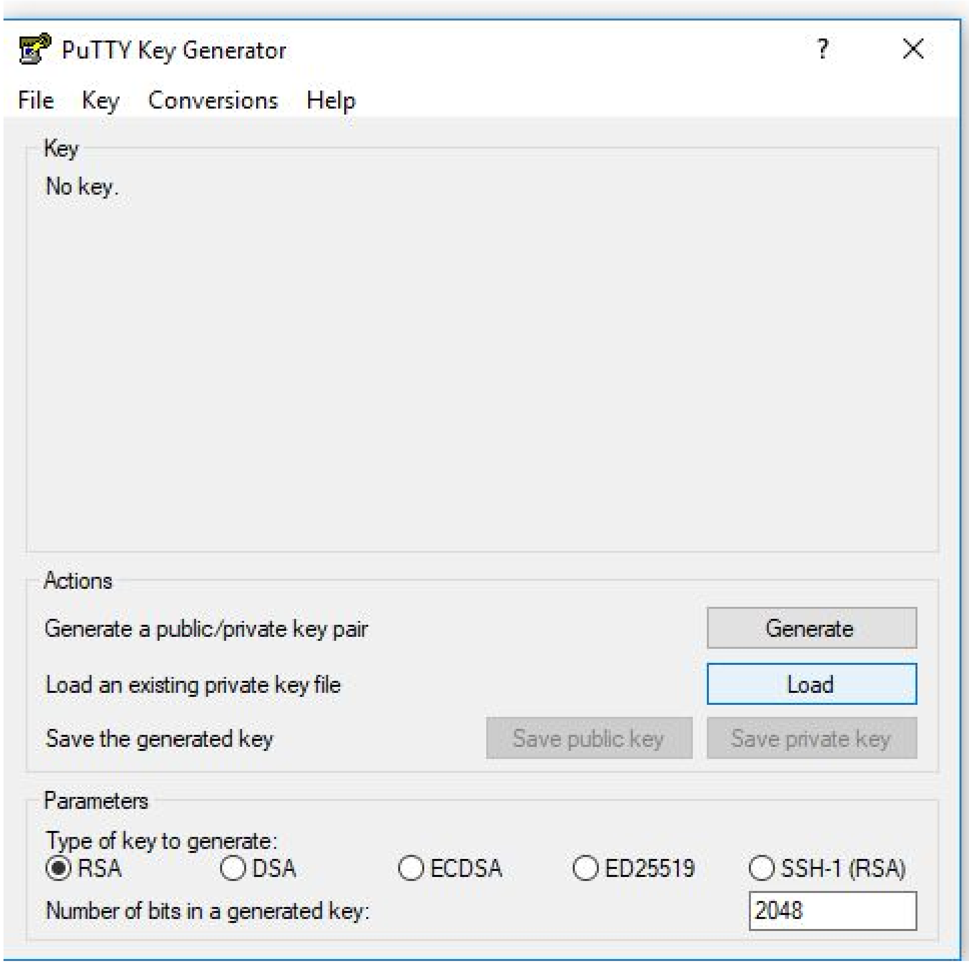
3. Run the installer in your machine. Follow the steps and you will have successfully installed both PuTTY and PuTTYgen in your machine.

4. Now, go to the 'Search' tab on your laptop and type 'putty'; the results will show

both PuTTY and PuTTYgen.



5. Windows doesn’t support .pem files and hence, PuTTYgen is used to convert .pem file to a .ppk file. To do this, **open PuTTYgen** and click on **‘Load’**.



Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

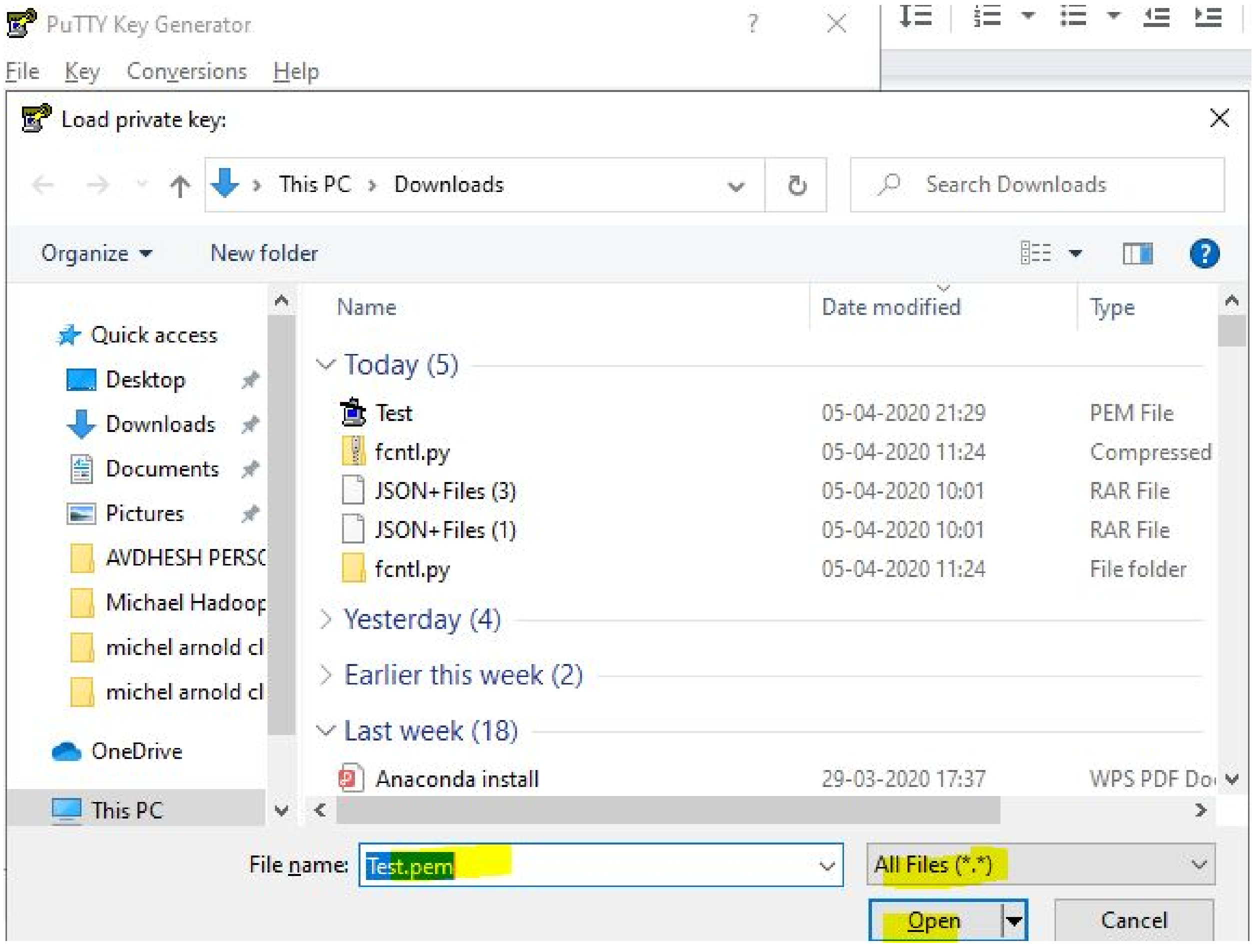
Save the generated key

Parameters

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

6. Locate the .pem file that you downloaded on your computer and select it. Do not forget to change the file type from .ppk to ‘**All files**’ to locate your **.pem file**.



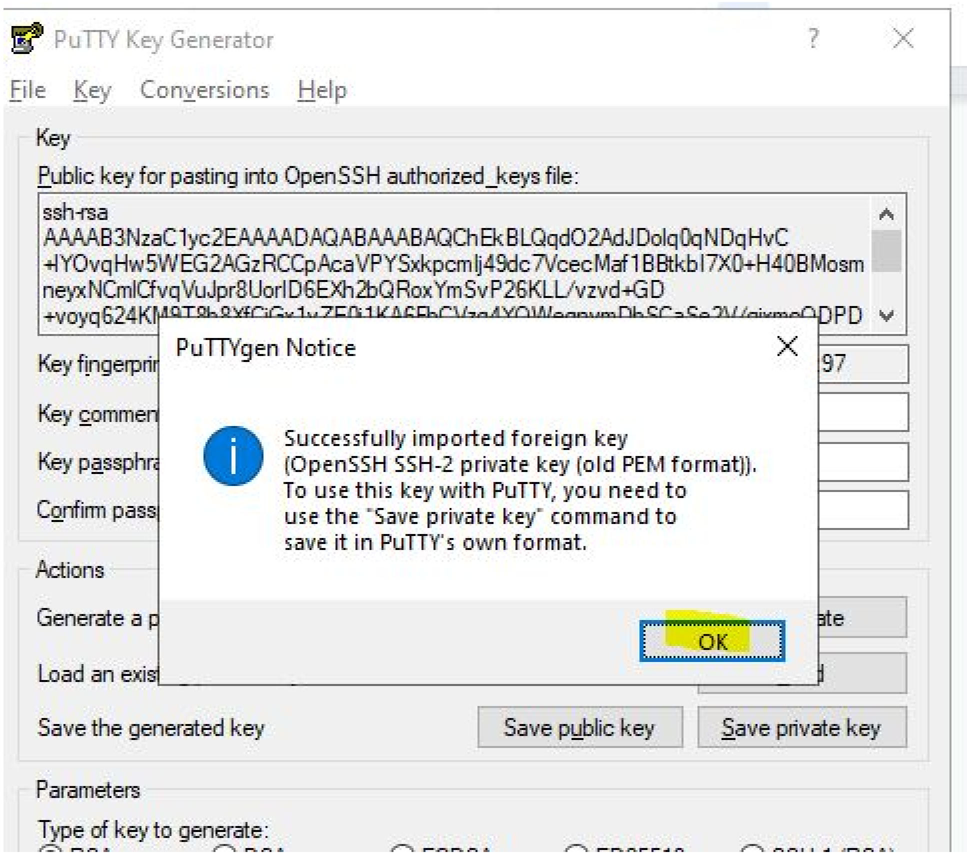
Load private key:

Name	Date modified	Type
Today (5)		
Test	05-04-2020 21:29	PEM File
fcntl.py	05-04-2020 11:24	Compressed
JSON+Files (3)	05-04-2020 10:01	RAR File
JSON+Files (1)	05-04-2020 10:01	RAR File
fcntl.py	05-04-2020 11:24	File folder
Yesterday (4)		
Earlier this week (2)		
Last week (18)		
Anaconda install	29-03-2020 17:37	WPS PDF Do

File name: Test.pem

All Files (*.*)

7. Click on **‘Open**’ and then click on **‘Ok’** on the pop up that appears on the screen.

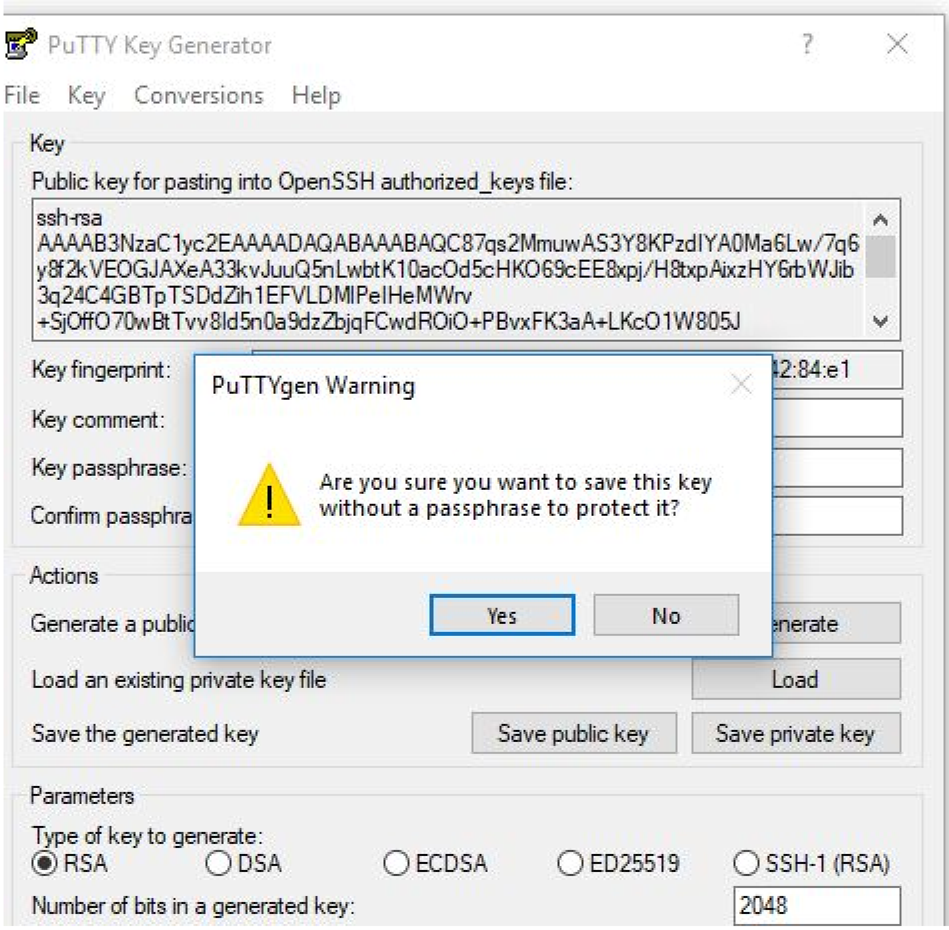


Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQChEkBLQqdO2AdJDolq0qNDqHvC
+lYOvqHw5WEG2AGzRCCpAcaVPYSxkpcmlj49dc7VcecMaf1BBtkbI7X0+H40BMosm
neyxNCmlCfvqVuJpr8UorlD6EXh2bQRoxYmSvP26KLL/vzvd+GD
+voyq624K
```

Successfully imported foreign key
(OpenSSH SSH-2 private key (old PEM format)).
To use this key with PuTTY, you need to
use the "Save private key" command to
save it in PuTTY's own format.

8. The **‘Key Passphrase**’ is an optional element. It will act as a password when you launch the instance using the ppk file. If you want to set a Key Passphrase, then remember to store it in a safe place. Click on ‘**Save private key’** and then click on **‘Yes’**.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC87qs2MmuwAS3Y8KPzdIYA0Ma6Lw/7q6
y8f2kVEOGJAXeA33kvJuuQ5nLwbtK10acOd5cHKO69cEE8xpj/H8txpAixzHY6rbWJib
3q24C4GBTpTSDdZih1EFVLDMIPeIHeMWrv
+SjOffO70wBtTvv8Id5n0a9dzZbjqFCwdROiO+PBvxFK3aA+LKcO1W805J
```

Key fingerprint: 12:84:e1

Key comment:

Key passphrase:

Confirm passphra

PuTTYgen Warning

Are you sure you want to save this key without a passphrase to protect it?

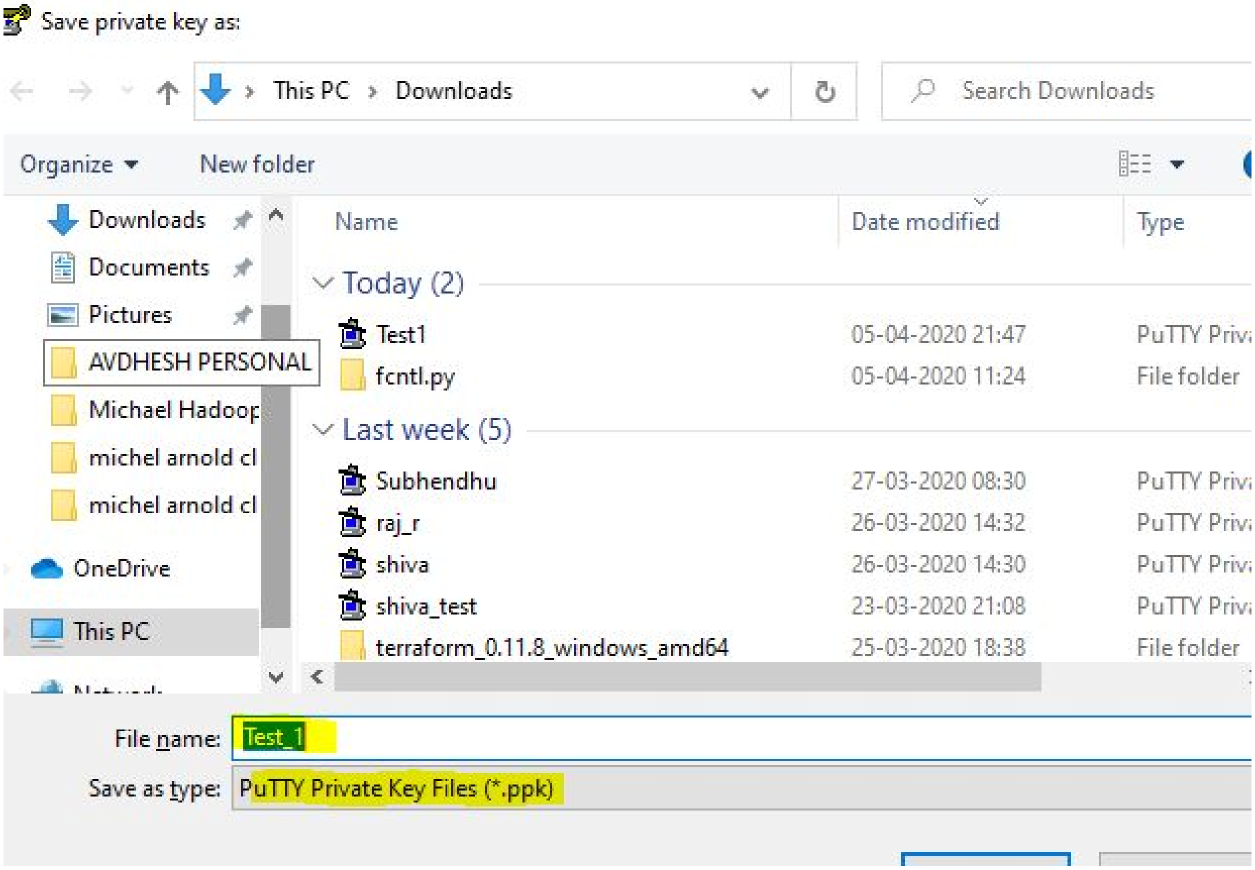
Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

9. Now, save your .ppk file in a safe location (**Test_1** in our case).

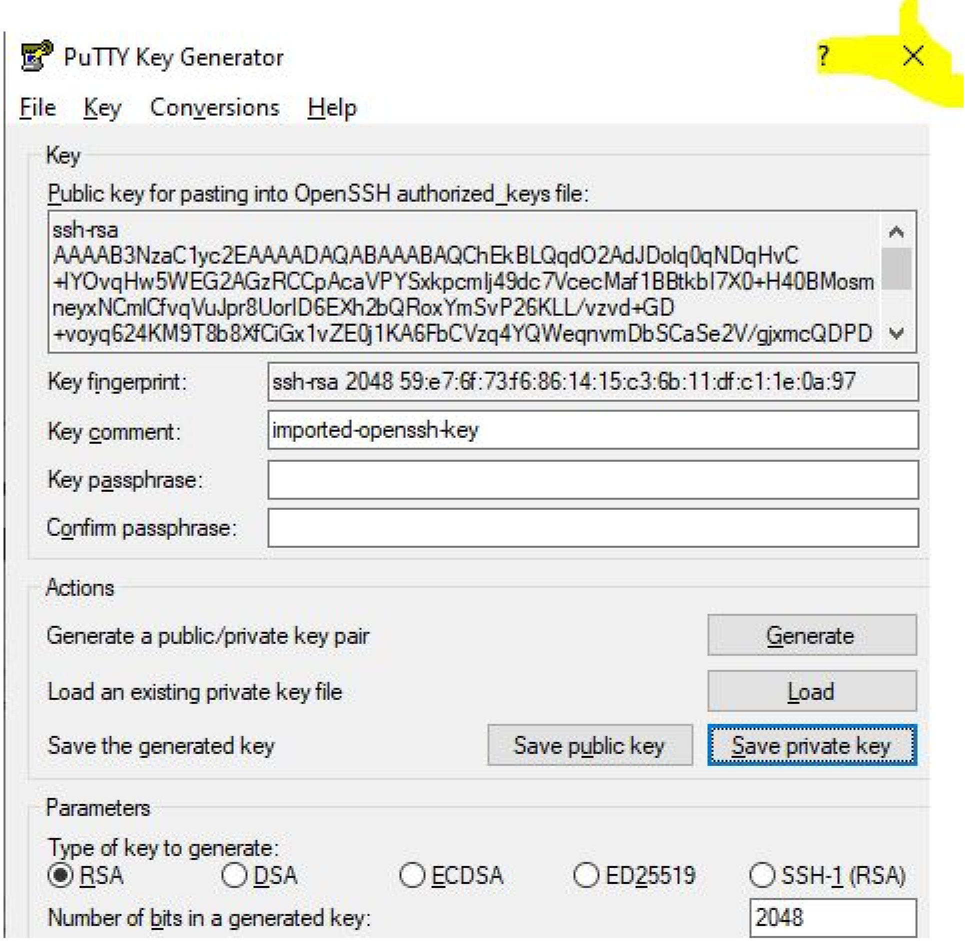


Name	Date modified	Type
Test1	05-04-2020 21:47	PuTTY Priv
fcntl.py	05-04-2020 11:24	File folder
Subhendhu	27-03-2020 08:30	PuTTY Priv
raj_r	26-03-2020 14:32	PuTTY Priv
shiva	26-03-2020 14:30	PuTTY Priv
shiva_test	23-03-2020 21:08	PuTTY Priv
terraform_0.11.8_windows_amd64	25-03-2020 18:38	File folder

File name: Test_1

Save as type: PuTTY Private Key Files (*.ppk)

10. You can close PuTTYgen now.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQChEkBLQqdO2AdJDolq0qNDqHvC
+lYOvqHw5WEG2AGzRCCpAcaVPYSxkpcmlj49dc7VcecMaf1BBtkbI7X0+H40BMosm
neyxNCmlCfvqVuJpr8UorID6EXh2bQRoxYmSvP26KLL/vzvd+GD
+voyq624KM9T8b8XfCiGx1vZE0j1KA6FbCVzq4YQWeqnvmDbSCaSe2V/gjxmcQDPD
```

Key fingerprint: ssh-rsa 2048 59:e7:6f:73:f6:86:14:15:c3:6b:11:df:c1:1e:0a:97

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

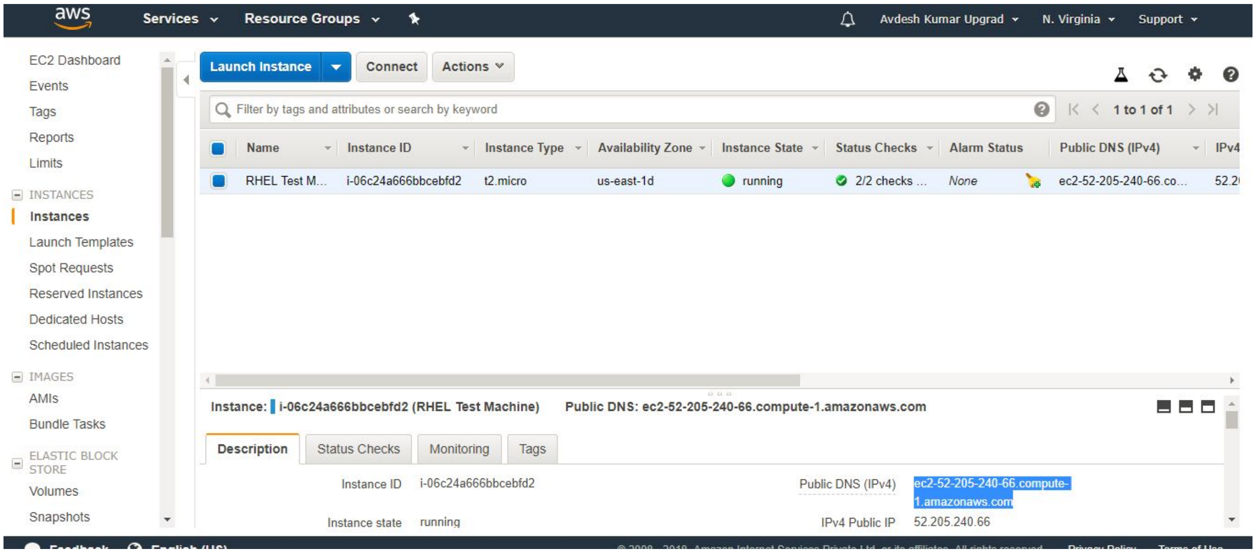
Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

11. Now, you need to open PuTTY to access the instance. But before that, open your EC2 dashboard and select your instance. Copy the '**Public DNS (IPv4)**' of your instance as shown below.

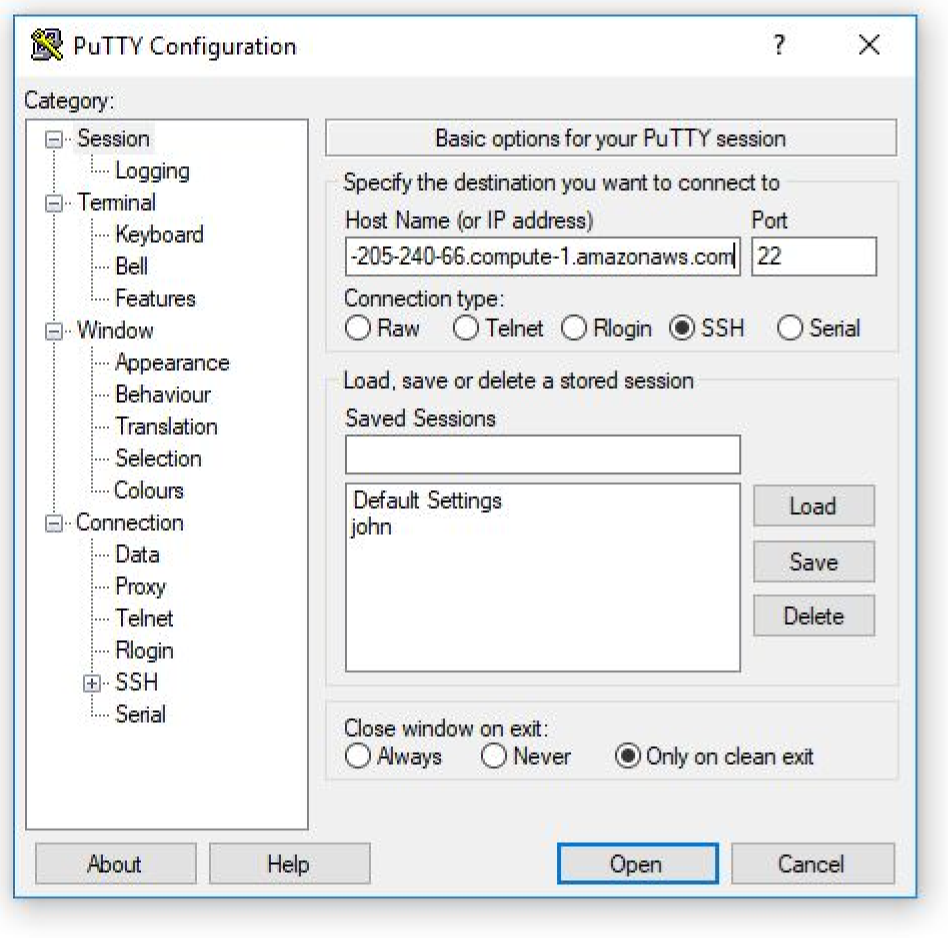


	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4
■	RHEL Test M...	i-06c24a666bbcebfd2	t2.micro	us-east-1d	● running	✓ 2/2 checks ...	None	ec2-52-205-240-66.co...	52.2

Instance: i-06c24a666bbcebfd2 (RHEL Test Machine) Public DNS: ec2-52-205-240-66.compute-1.amazonaws.com

Instance ID	i-06c24a666bbcebfd2	Public DNS (IPv4)	ec2-52-205-240-66.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	52.205.240.66

12. Now, open PuTTY. Paste the copied information under the **‘Host Name’** section of the PuTTY window.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): -205-240-66.compute-1.amazonaws.com

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

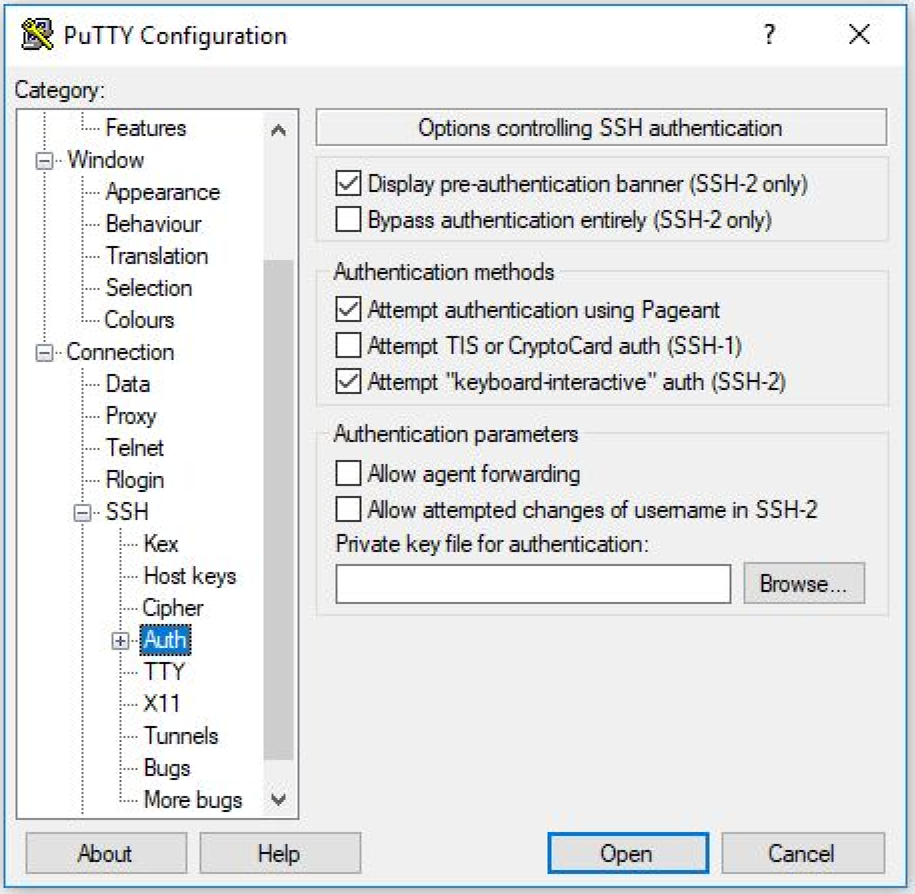
Load, save or delete a stored session

Saved Sessions

Default Settings
john

Close window on exit: ○ Always ○ Never ● Only on clean exit

13. On the left-hand side panel, click on **'Connection'**. Then click on **'SSH'** followed by **'Auth'**. You will find the space to provide the In the private key file. Here, click on the **'Browse'** button and select the .ppk file (**Test_1.ppk**) that you generated using PuTTYgen above.



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

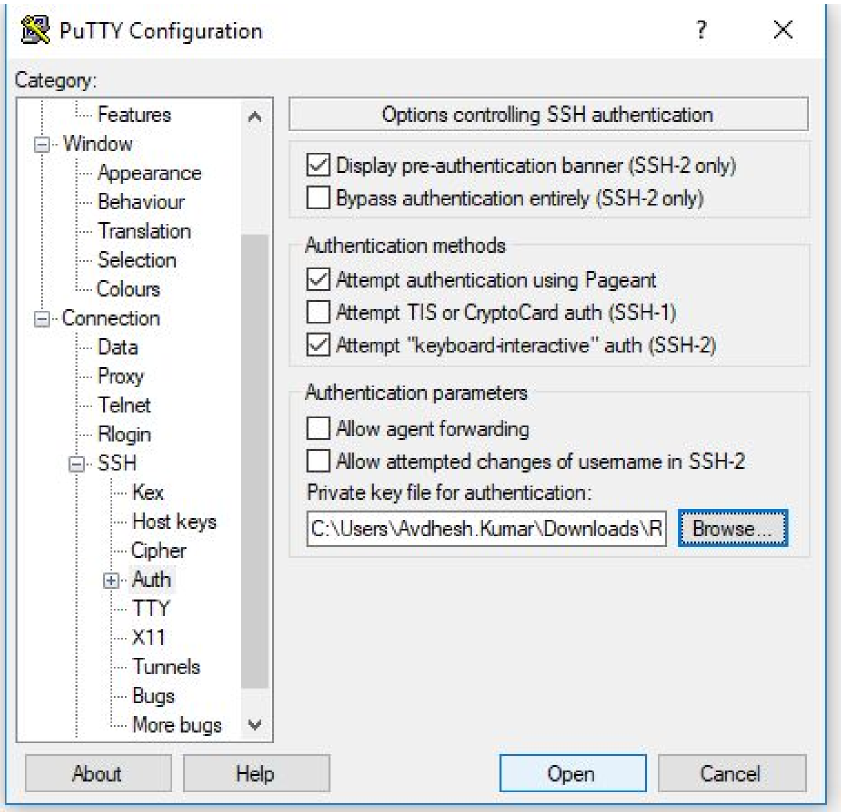
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

Browse...



Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
□ Bypass authentication entirely (SSH-2 only)

Authentication methods

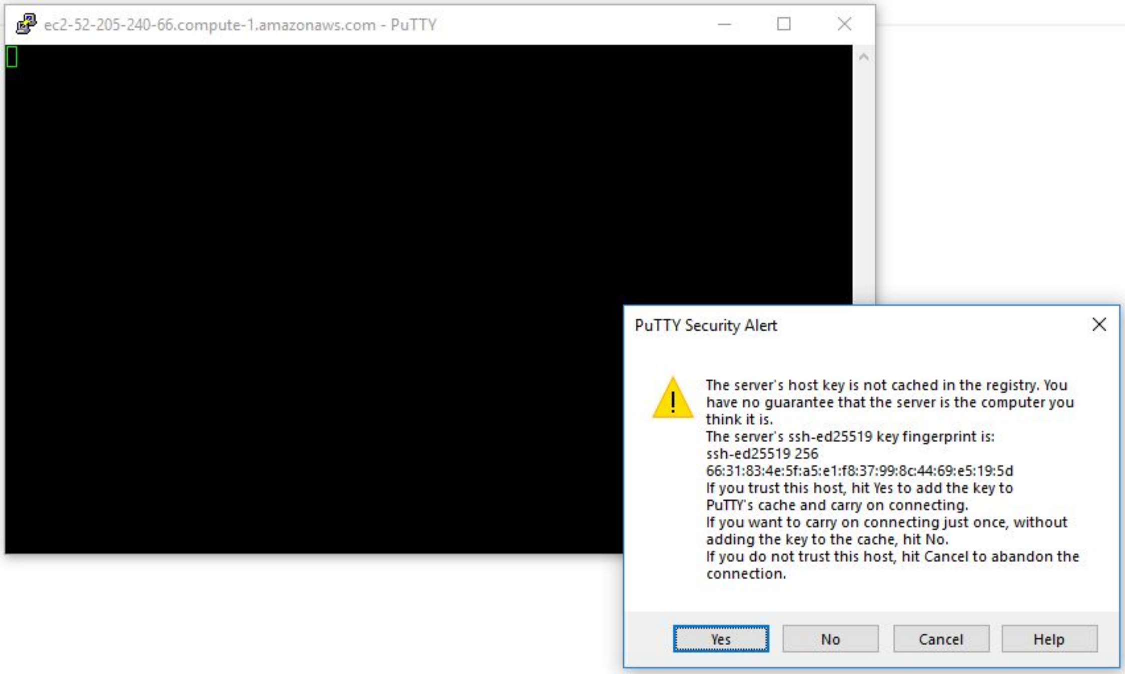
☑ Attempt authentication using Pageant
□ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding
□ Allow attempted changes of username in SSH-2

Private key file for authentication:
C:\Users\Avdhesh.Kumar\Downloads\R Browse...

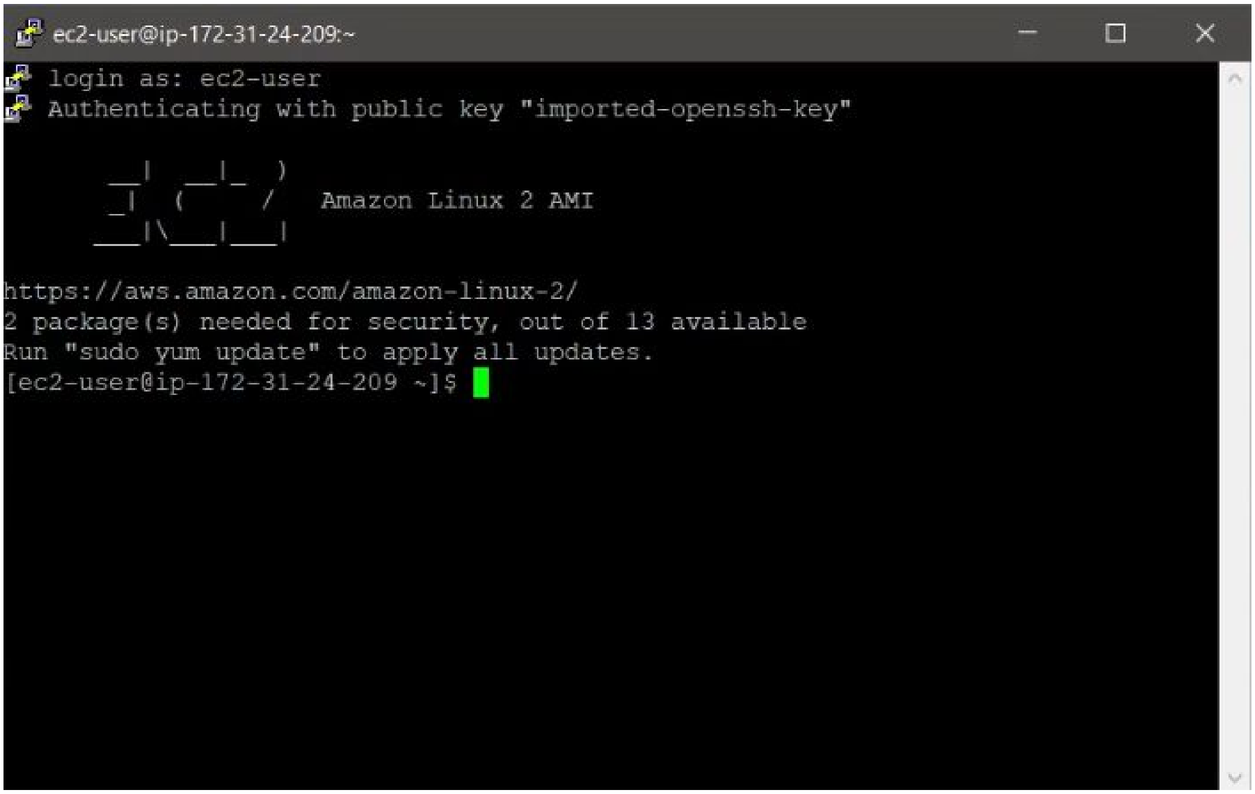
14. Click on ‘**Open**’. If you have provided correct IP under the Security Groups, you will receive a window prompt. Press **‘Yes’**. and login with the user as **ec2-user**.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256
66:31:83:4e:5f:a5:e1:f8:37:99:8c:44:69:e5:19:5d
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

(If you have added a security keyphrase, you will have to provide that to login.)

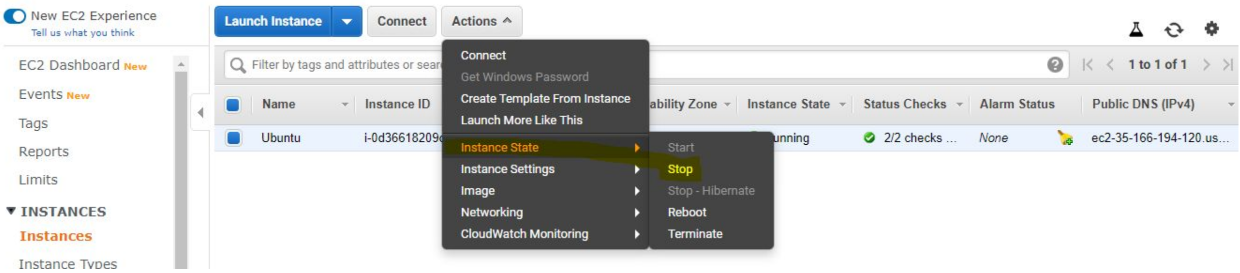


```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 13 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-24-209 ~]$
```

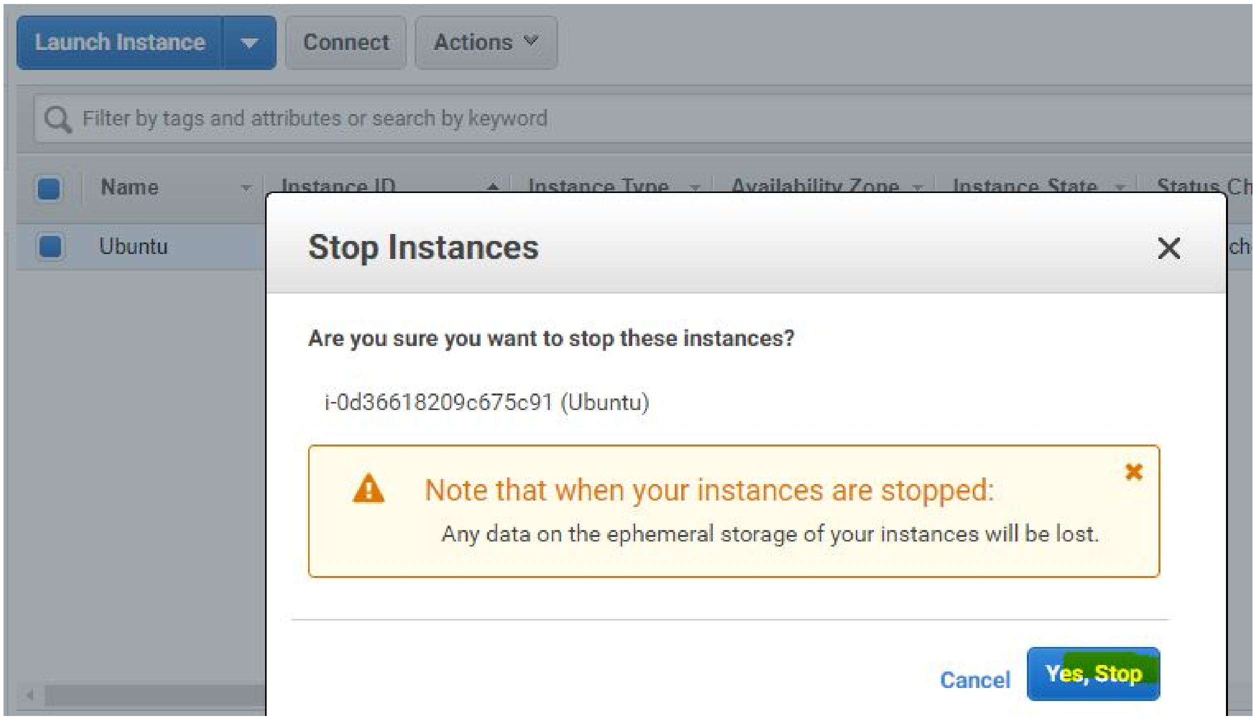
15. Now, your local machine has successfully established a connection with the EC2 Instance.

NOTE-: After you have created the instance, please stop the t2.micro instance when your work is over. Otherwise, your credits will get deducted. The steps to stop the instance are given below:

1. Go to your EC2 dashboard and select your ec2 instance then click to “Action” > Instance State > Stop



2. Click on **Yes.Stop.**



Stop Instances

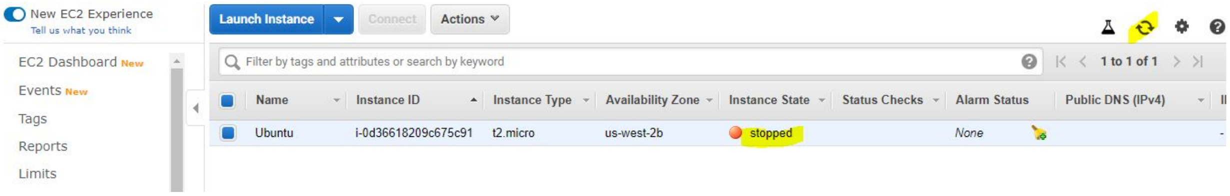
Are you sure you want to stop these instances?

i-0d36618209c675c91 (Ubuntu)

Note that when your instances are stopped:

Any data on the ephemeral storage of your instances will be lost.

3. Verify with Instance state.it should be stopped state and colour state is Red.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	I
Ubuntu	i-0d36618209c675c91	t2.micro	us-west-2b	🔴 stopped		None		-

For Linux/Mac OS users to connect to the EC2 Instance.

For Linux/Mac systems, **you don't need to convert your .pem file to a .ppk file**.

1. Open **'Terminal'** on your system and go to the location where you downloaded the **.pem file**.

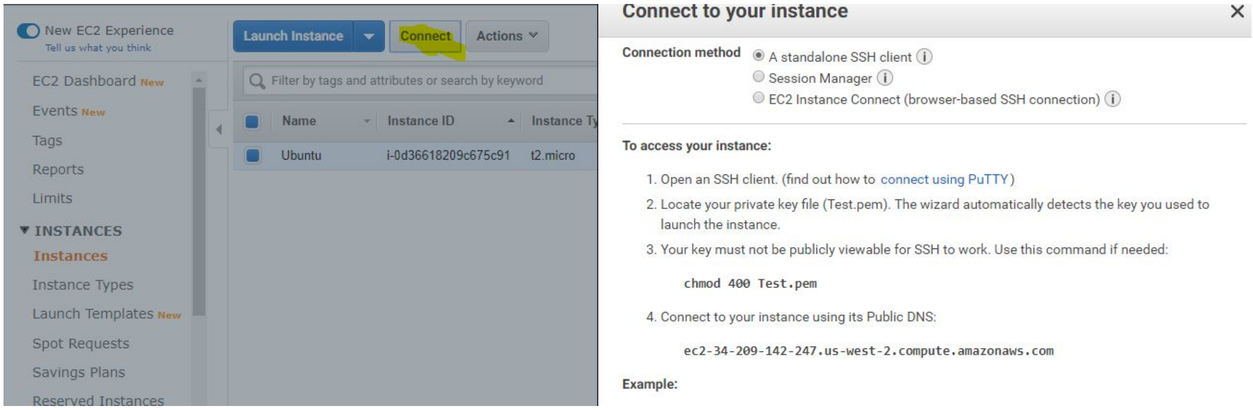
   Let's say that your .pem file was downloaded in the 'Downloads' folder. You need to first change your current working directory to the 'Downloads' directory. To do that, use the following '**cd**' command: **cd ./Downloads/**

2. Next, run the ' **ls** ' command, which lists all the files in a given Linux directory. Verify that your .pem file exists in the given directory.

3. Change the permissions of the .pem file to 400, which gives the read permission and removes all other permissions from the user. The command is shown below. (Test.pem is the filename in our case.)

   chmod 400 Test.pem

4. Now, go back to your EC2 instance page and click on the 'Connect' button to get the command for the connection. After clicking, you will see the following screen appear.



Connect to your instance

Connection method ● A standalone SSH client ⓘ
○ Session Manager ⓘ
○ EC2 Instance Connect (browser-based SSH connection) ⓘ

To access your instance:

1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (Test.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 Test.pem
```

4. Connect to your instance using its Public DNS:

```
ec2-34-209-142-247.us-west-2.compute.amazonaws.com
```

Example:

5. Use the command shown under ‘Example’ on your screen to connect to the instance. The command is

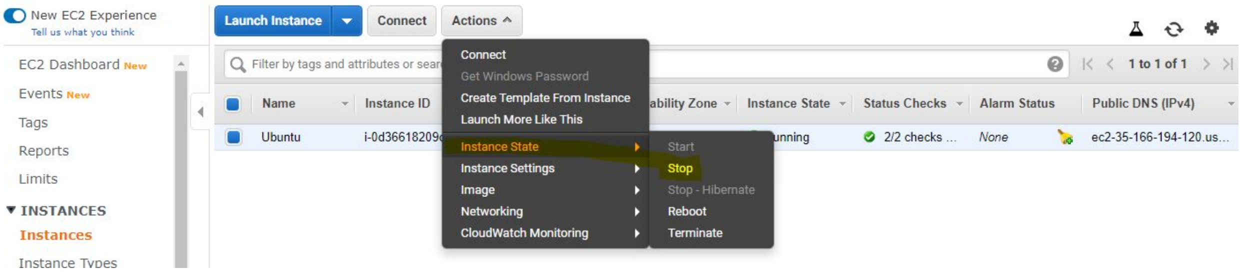
   ssh -i Test.pem ubuntu@public_dns_name

   Replace the public_dns_name with your own public DNS name. Also, before running this command, ensure that you are present in the directory in which your .pem file is present. This can be checked using the ‘ **pwd** ’ command, which writes the full path of the current working directory.

6. If you have provided correct IP under the Security Groups, you will receive a window prompt. Type **‘Yes’**. inside the terminal and press Enter. Instance will be launched.

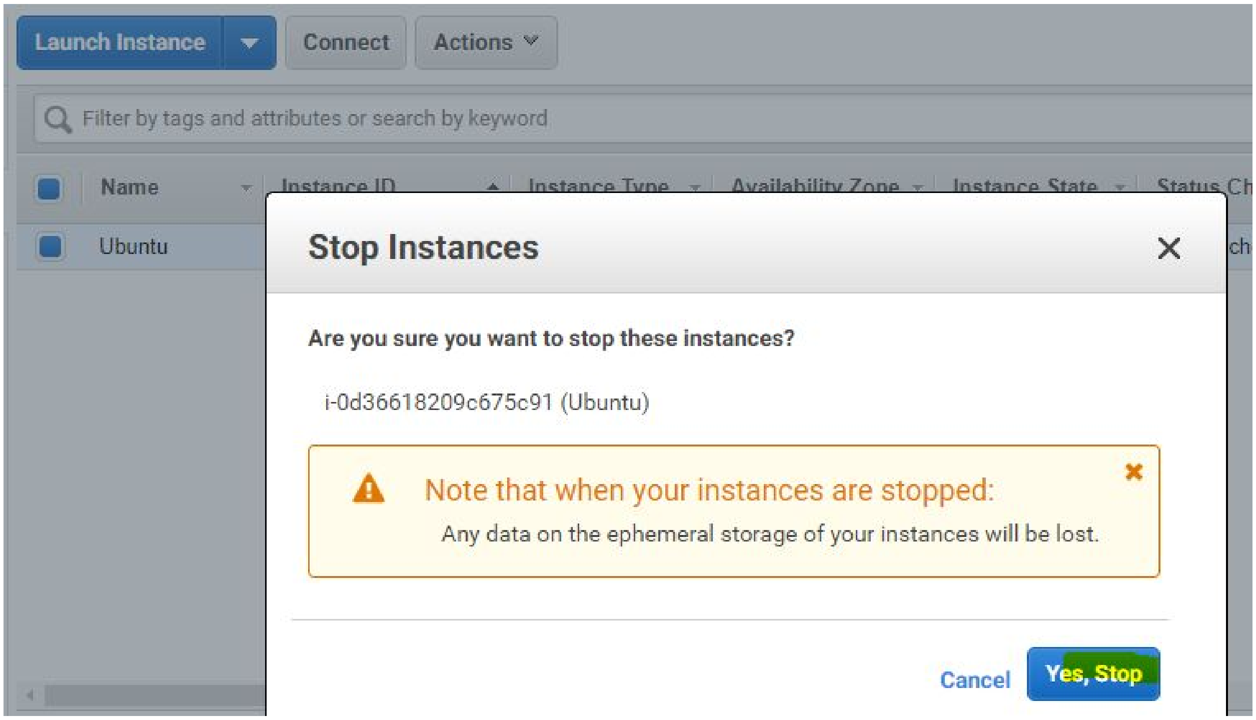
NOTE-: After you have created the instance, please stop the t2.micro instance when your work is over. Otherwise, your credits will get deducted. The steps to stop the instance are given below:

1. Go to your EC2 dashboard and select your ec2 instance then click to “Action” > Instance State > Stop



Name	Instance ID	ability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Ubuntu	i-0d36618209		unning	2/2 checks ...	None	ec2-35-166-194-120.us...

2. Click on **Yes.Stop.**



Stop Instances

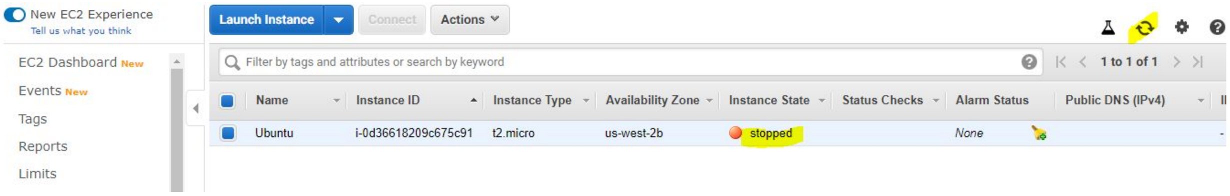
Are you sure you want to stop these instances?

i-0d36618209c675c91 (Ubuntu)

Note that when your instances are stopped:

Any data on the ephemeral storage of your instances will be lost.

3. Verify with Instance state.it should be stopped state and colour state is Red.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Ubuntu	i-0d36618209c675c91	t2.micro	us-west-2b	● stopped		None	-