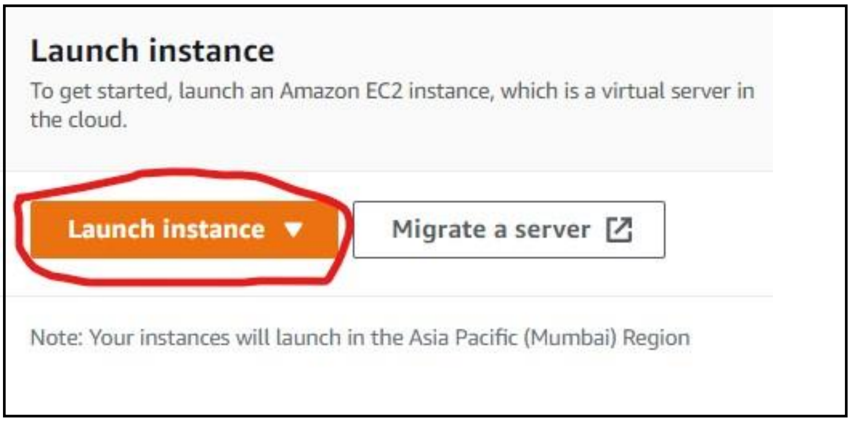
Title: Live Vue.js Front-end (quasar project) project in Aws Ec2-Instance.

Step1: Open Ec2 and launch instance using option “Launch Instance.”

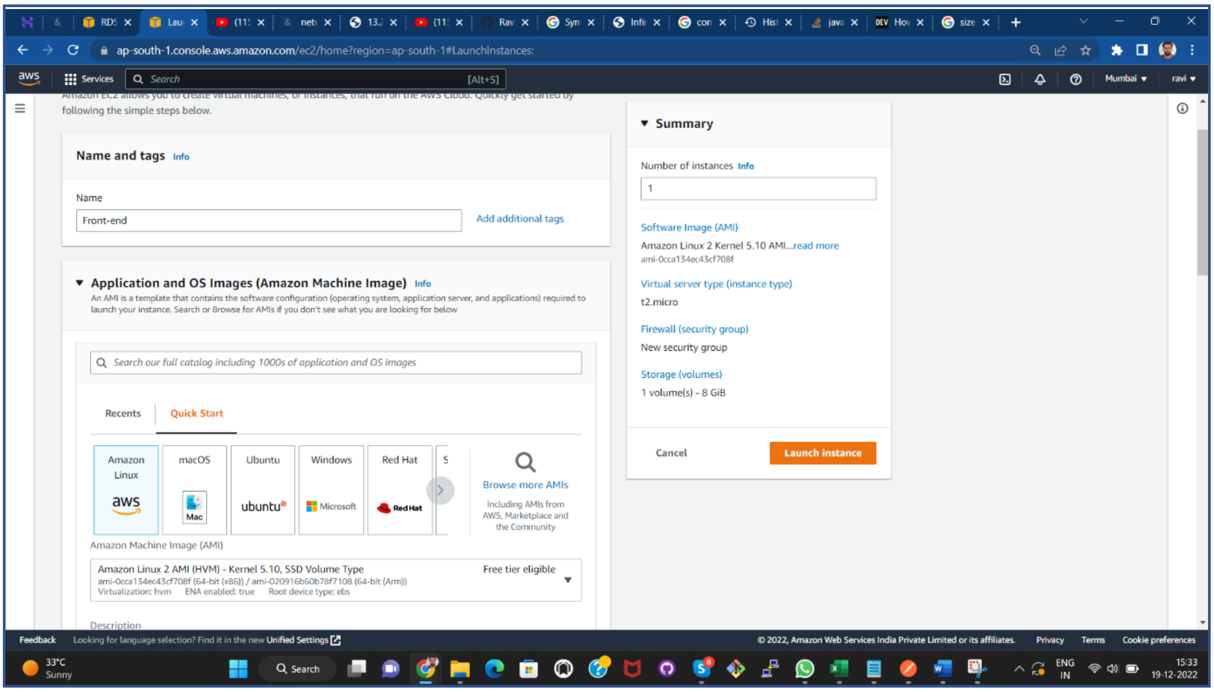


Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Asia Pacific (Mumbai) Region

Step2: Give name that instance what you want and select ‘Amazon Linux’ OS in “**Application and OS Images (Amazon Machine Image)**” option.



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Front-end

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible
ami-0cca134ec43cf708f (64-bit (x86)) / ami-020916b60b78f7108 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more ami-0cca134ec43cf708f

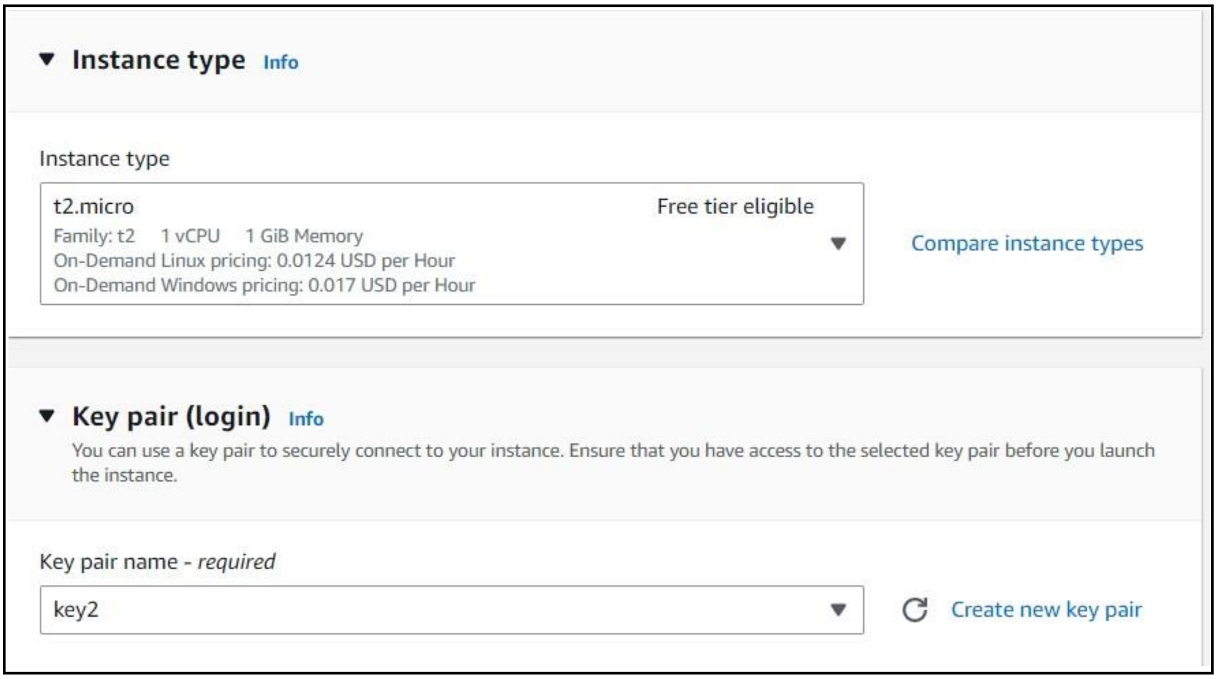
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

aws
Services
Search
[Alt+S]
Mumbai ▾
ravi ▾
Add additional tags
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Cancel
Launch instance
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
33°C Sunny
ENG IN
15:33
19-12-2022

Step3: Select Instance Type (Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and **give you the flexibility to choose the appropriate mix of resources for your applications**.) as per your website requirement, then select “key pair(login)” if you have one or create new one using “create new key pair” option.



▼ **Instance type** Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0124 USD per Hour
On-Demand Windows pricing: 0.017 USD per Hour

▼ **Key pair (login)** Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

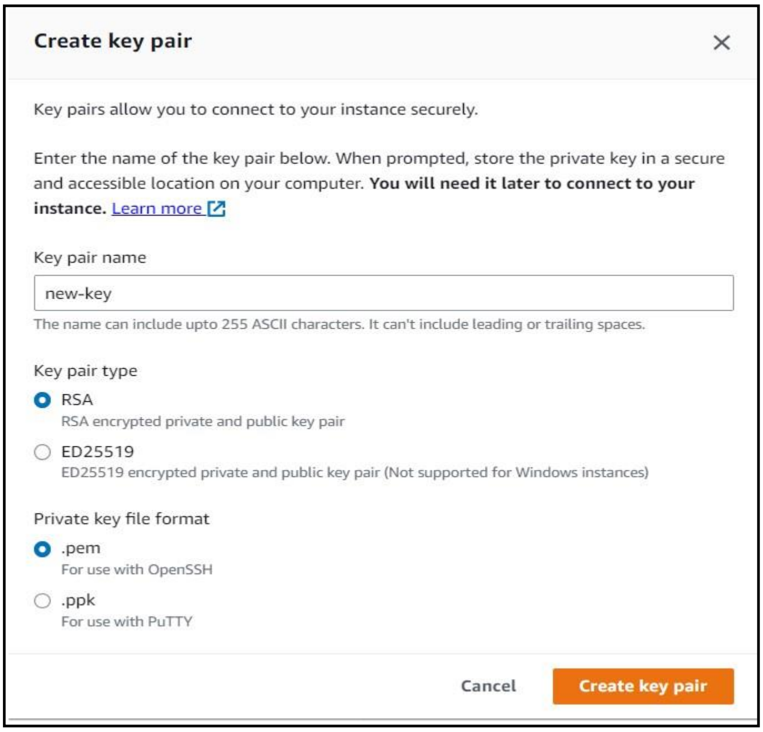
Key pair name - *required*

key2

==

- **How to create Key pair.**

Select "create new key pair" option, then name it and select options for "Key pair type" and "Private key file format" as shown in following image. Next, click "Create key pair" option, your new key is now generated.



Create key pair

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Key pair name

new-key

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

○ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

● .pem
For use with OpenSSH

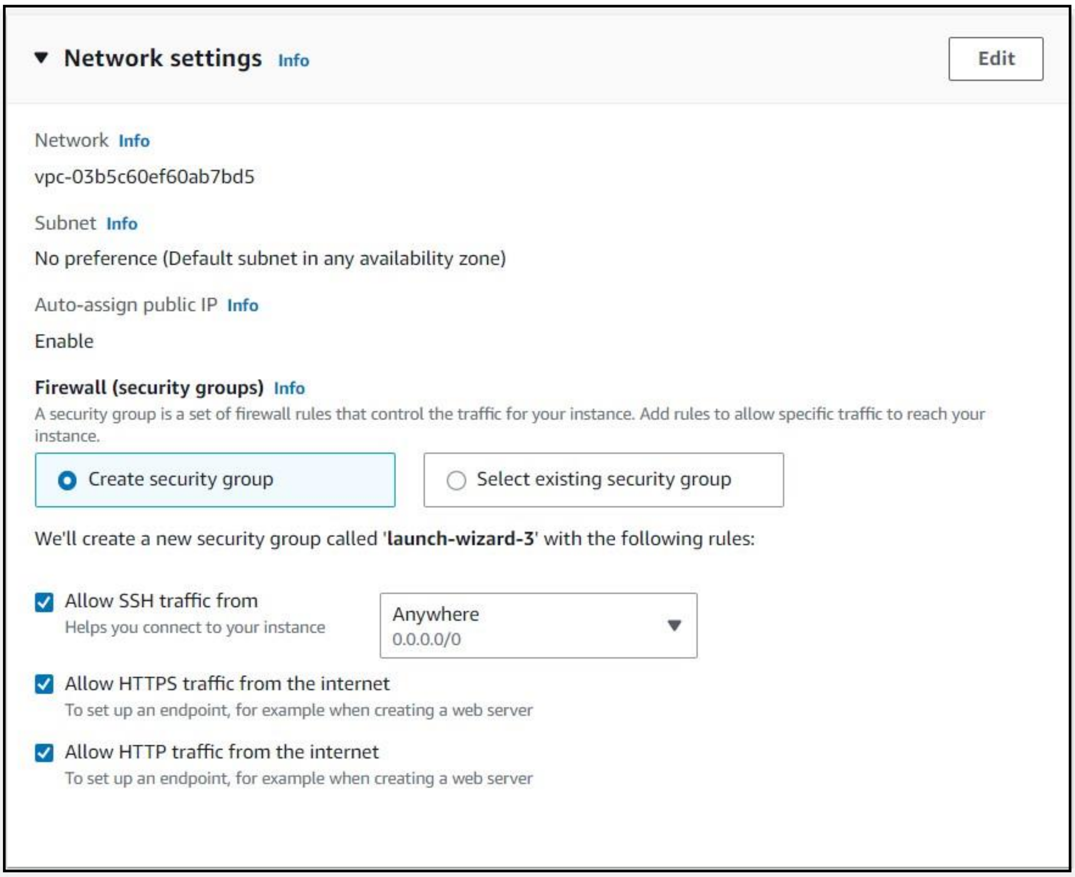
○ .ppk
For use with PuTTY

==

Step4:

Network setting> Firewall (security groups) select "**Create security group**" if you don't have one or if you already created security group select "**Select existing security group**" and then select the name of security group you created.

For "**Create security group**" option select check-box of "**Allow SSH traffic from, Allow HTTPS traffic from the internet, Allow HTTP traffic from the internet**".



▼ Network settings Info

Network Info
vpc-03b5c60ef60ab7bd5

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-3**' with the following rules:

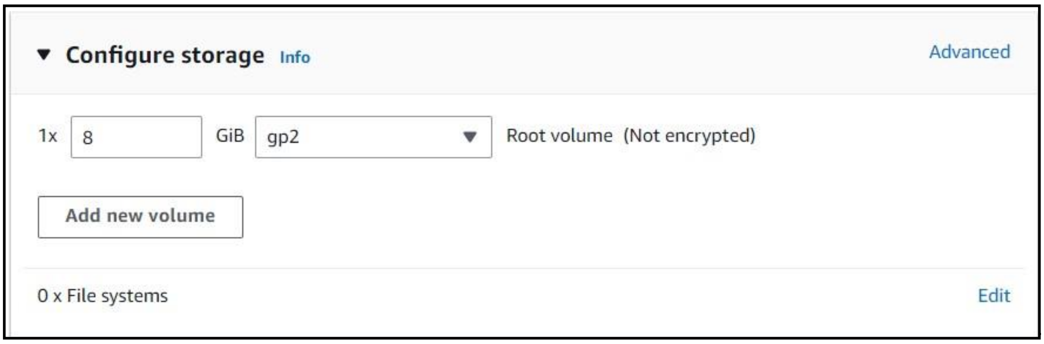
☑ Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

Step5:

In "**Configure Storage"** select size of storage as per limitation of EBS volume type. (Here I take 8gb in **gb2** EBS volume type, which's limitation is up to 30gb for free tier eligible account.)



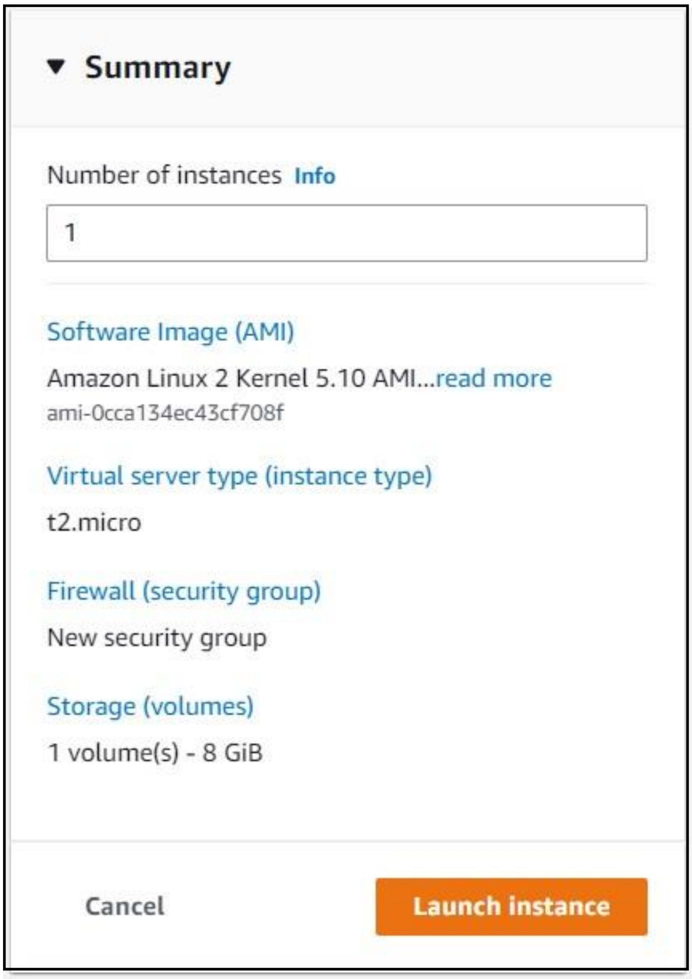
▼ Configure storage Info

1x 8 GiB gp2 Root volume (Not encrypted)

0 x File systems

Step6:

Select **“Launch instance”** and launch it.



▼ Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-0cca134ec43cf708f

Virtual server type (instance type)

t2.micro

Firewall (security group)

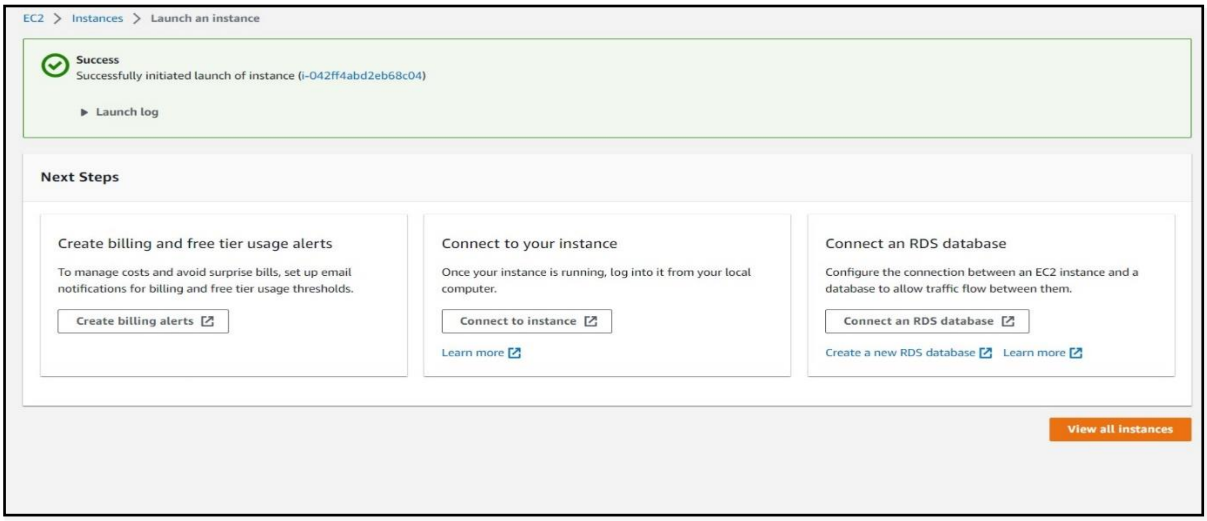
New security group

Storage (volumes)

1 volume(s) - 8 GiB

Step7:

Choose “**view all instances**”



EC2 > Instances > Launch an instance

Success

Successfully initiated launch of instance (i-042ff4abd2eb68c04)

▶ Launch log

Next Steps

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance

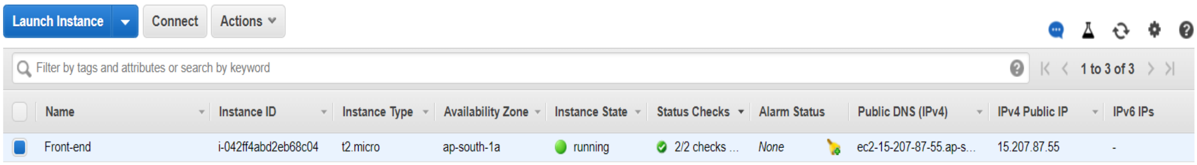
Once your instance is running, log into it from your local computer.

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Step8:

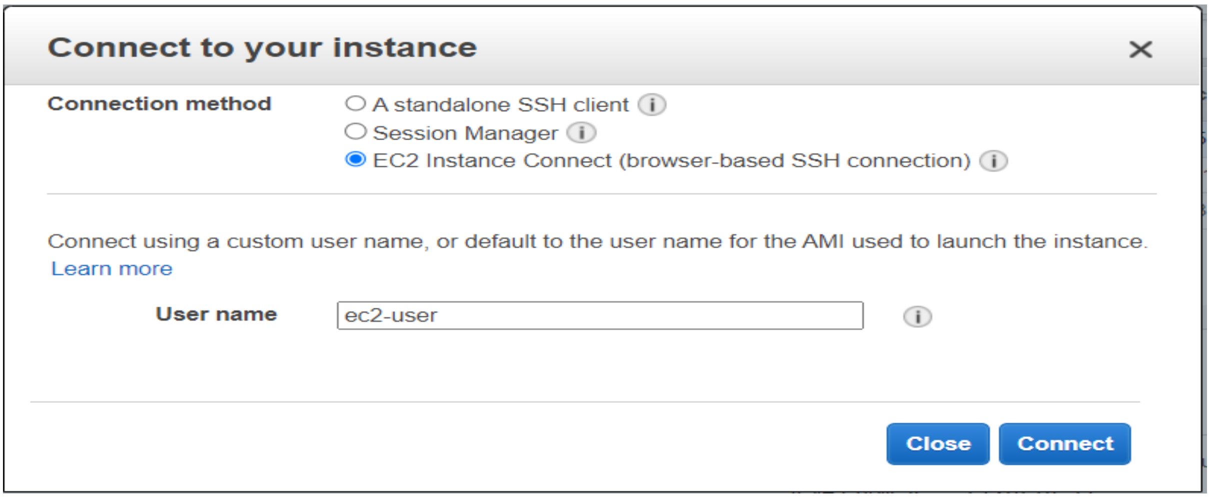
Choose Option “**Connect**” after the “**Status Checks**” shows “**2/2checks**”.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
Front-end	i-042ff4abd2eb68c04	t2.micro	ap-south-1a	● running	✓ 2/2 checks ...	None	ec2-15-207-87-55.ap-s...	15.207.87.55	-

Step9:

Choose “**EC2 Instance Connect (browser-based SSH connection)**” and select “Connect” option.



Connect to your instance

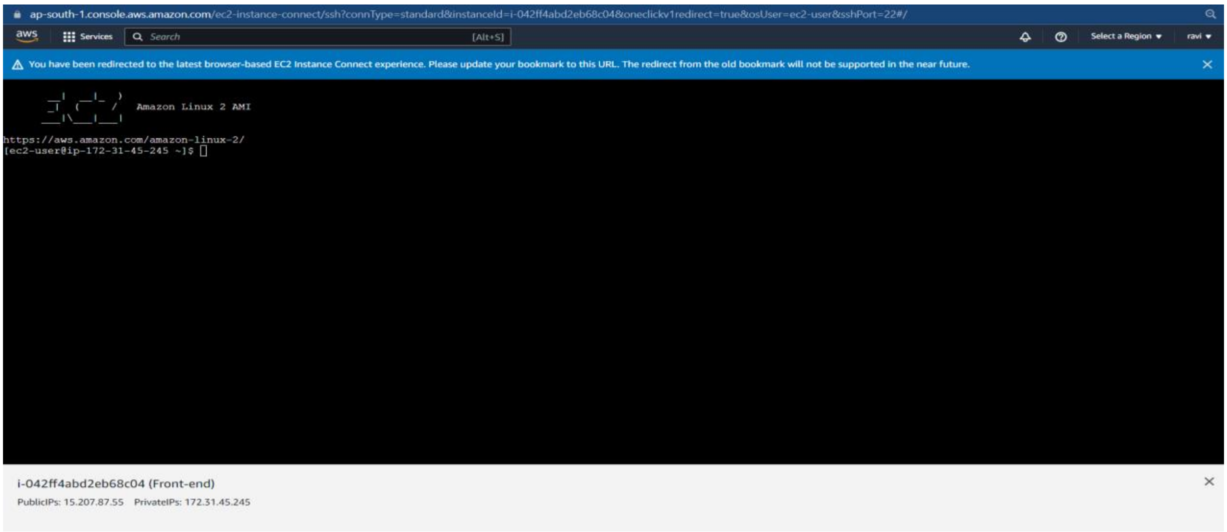
Connection method
○ A standalone SSH client
○ Session Manager
● EC2 Instance Connect (browser-based SSH connection)

Connect using a custom user name, or default to the user name for the AMI used to launch the instance.
Learn more

User name: ec2-user

Step 10:

This type of interface is open.



ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-042ff4abd2eb68c04&oneclickv1redirect=true&osUser=ec2-user&sshPort=22#/

You have been redirected to the latest browser-based EC2 Instance Connect experience. Please update your bookmark to this URL. The redirect from the old bookmark will not be supported in the near future.

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-45-245 ~]$ 
```

i-042ff4abd2eb68c04 (Front-end)
PublicIPs: 15.207.87.55 PrivateIPs: 172.31.45.245

Now, first give following cmds :

sudo su

sudo yum update

- Install git using cmd:

sudo yum install git -y

- Active git using following cmd:

git init

- Create ssh key using following cmd in terminal

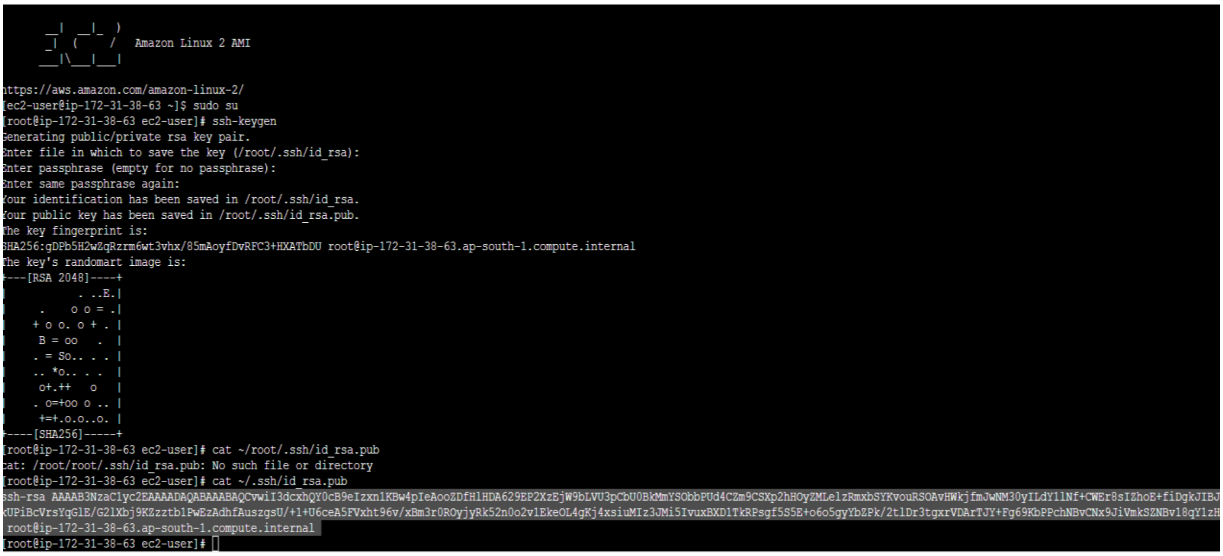
ssh-keygen

or

ssh-keygen -t ed25519 -C "mailto:youremailaddress@domain.tld DAY-MONTH-YEAR" -f ~/.ssh/my_key

- Use below shown cmd and then copy “id_rsa.pub” text data which have been shown below:

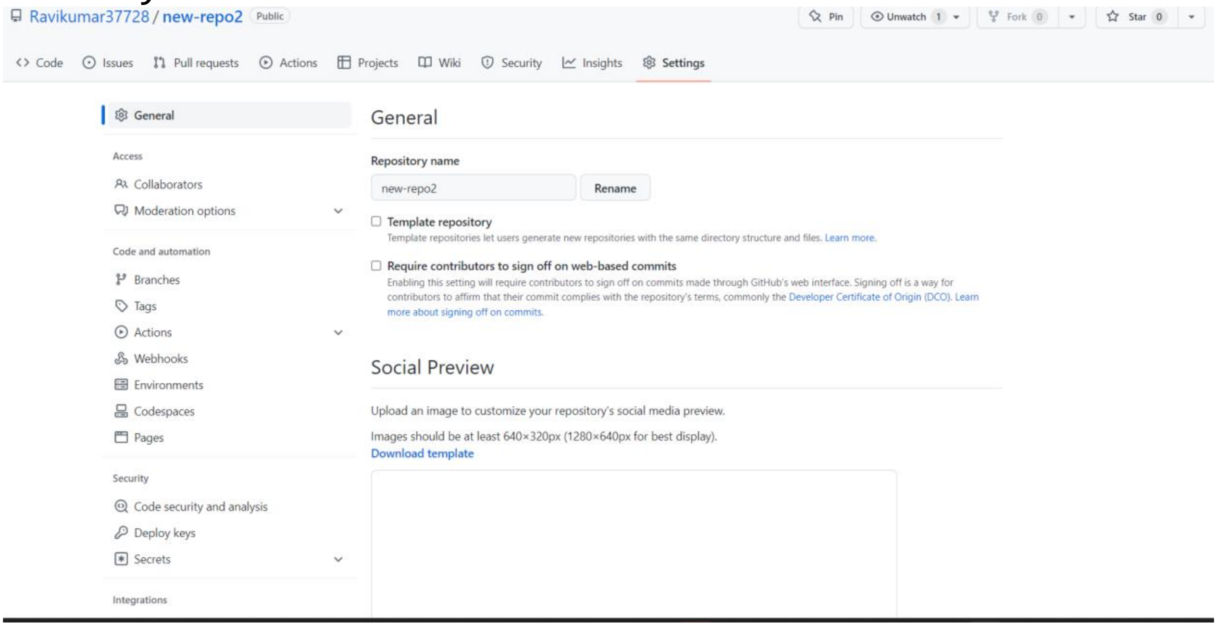
cat ~/.ssh/id_rsa.pub



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

ttps://aws.amazon.com/amazon-linux-2/
ec2-user@ip-172-31-38-63 ~]$ sudo su
root@ip-172-31-38-63 ec2-user]# ssh-keygen
enerating public/private rsa key pair.
nter file in which to save the key (/root/.ssh/id_rsa):
nter passphrase (empty for no passphrase):
nter same passphrase again:
our identification has been saved in /root/.ssh/id_rsa.
our public key has been saved in /root/.ssh/id_rsa.pub.
he key fingerprint is:
HA256:gDPb5H2wZqRzrm6wt3vhx/85mAoyfDvRFC3+HXATbDU root@ip-172-31-38-63.ap-south-1.compute.internal
he key's randomart image is:
---[RSA 2048]----+
          . ..E.|
   .    o o = .|
  + o o. o + . |
   B = oo   .  |
  . = So.. . . |
  .. *o.. . .  |
   o+.++   o   |
  . o=+oo o .. |
   +=+.o.o..o. |
----[SHA256]-----+
root@ip-172-31-38-63 ec2-user]# cat ~/root/.ssh/id_rsa.pub
at: /root/root/.ssh/id_rsa.pub: No such file or directory
root@ip-172-31-38-63 ec2-user]# cat ~/.ssh/id_rsa.pub
sh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCvwiI3dcxhQY0cB9eIzxn1KBw4pIeAooZDfHlHDA629EP2XzEjW9bLVU3pCbU0BkMmYSObbPUd4CZm9CSXp2hHOyZMLelzRmxbSYKvouRSOAvHWkjfmJwNM30yILdY1lNf+CWEr8sIZhoE+fiDgkJIBJ
UPiBcVrsYqGlE/G2lXbj9KZzztb1PwEzAdhfAuszgsU/+1+U6ceA5FVxht96v/xBm3r0ROyjyRk52n0o2v1EkeOL4gKj4xsiuMIz3JMi5IvuxBXD1TkRPsgf5S5E+o6o5gyYbZPk/2tlDr3tgxrVDArTJY+Fg69KbPPchNBvCNx9JiVmkSZNBv18qY1zH
 root@ip-172-31-38-63.ap-south-1.compute.internal
root@ip-172-31-38-63 ec2-user]# 
```

- Paste it in git-hub source code repo.>settings>Deploy Keys.



General

Repository name

new-repo2 Rename

□ Template repository

Template repositories let users generate new repositories with the same directory structure and files. Learn more.

□ Require contributors to sign off on web-based commits

Enabling this setting will require contributors to sign off on commits made through GitHub's web interface. Signing off is a way for contributors to affirm that their commit complies with the repository's terms, commonly the Developer Certificate of Origin (DCO). Learn more about signing off on commits.

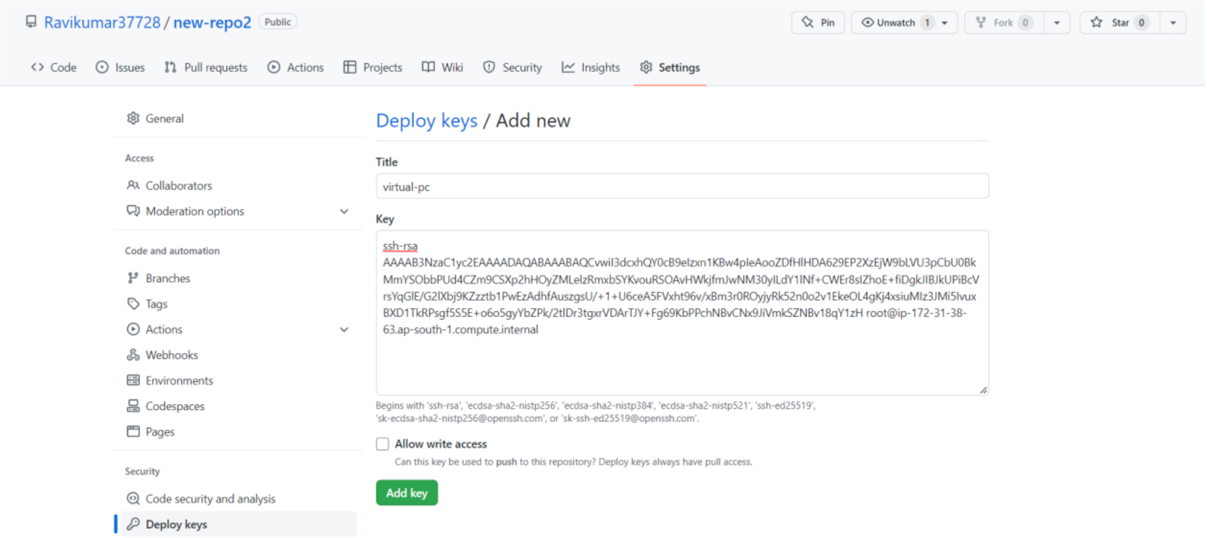
Social Preview

Upload an image to customize your repository's social media preview.

Images should be at least 640×320px (1280×640px for best display).

Download template

- Paste copied text in there and named it.then press “Add key”



Deploy keys / Add new

Title

virtual-pc

Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvwil3dcxhQY0cB9eIzxn1KBw4pleAooZDfHlHDA629EP2XzEjW9bLVU3pCbU0Bk
MmYSObbPUd4CZm9CSXp2hHOyZMLelzRmxbSYKvouRSOAvHWkjfmJwNM30yILdY1lNf+CWEr8sIZhoE+fiDgkJIBJkUPiBcV
rsYqGlE/G2lXbj9KZzztb1PwEzAdhfAuszgsU/+1+U6ceA5FVxht96v/xBm3r0ROyjyRk52n0o2v1EkeOL4gKj4xsiuMIz3JMi5lvux
BXD1TkRPsgf5S5E+o6o5gyYbZPk/2tlDr3tgxrVDArTJY+Fg69KbPPchNBvCNx9JiVmkSZNBv18qY1zH root@ip-172-31-38-
63.ap-south-1.compute.internal
```

Begins with 'ssh-rsa', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'ssh-ed25519', 'sk-ecdsa-sha2-nistp256@openssh.com', or 'sk-ssh-ed25519@openssh.com'.

□ Allow write access

Can this key be used to **push** to this repository? Deploy keys always have pull access.

Add key

Your key is ssh key is now added in git hub repo.

Step 11:

- Give following cmd for activate github repo in ec2.

ssh git@github.com

- Type “yes” in connecting

- Now git hub is successfully connect to your ec2 insatnces.
- Now add ssh link in your following cmd in terminal
  git remote add origin (ssh link)
  e.g.
  git remote add origin git@github.com:Ravikumar37728/new-repo2.git

- Now use following cmd for pull codes in ec2.

  git pull origin Master

  or

  git pull origin main

  //main or master or other branch is depended upon which branch code you want to pull from git-hub repo.

- Give following cmds:

```
sudo su

curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.34.0/install.sh | bash

. ~/.nvm/nvm.sh

nvm install 16

npm i npm@latest -g

npm install --legacy-peer-deps

npm i @vue/cli-service --legacy-peer-deps
```

- after it just fire following cmd for run and live the website, even terminal is turnoff.

```
screen -d -m npx quasar dev
```

- now, run IPv4 Public IP in browser,your project is live on it.

NOTE: if you stop the instance in any case and restart it then fire “screen -d -m npx quasar dev” cmd again before going live again for make it live.