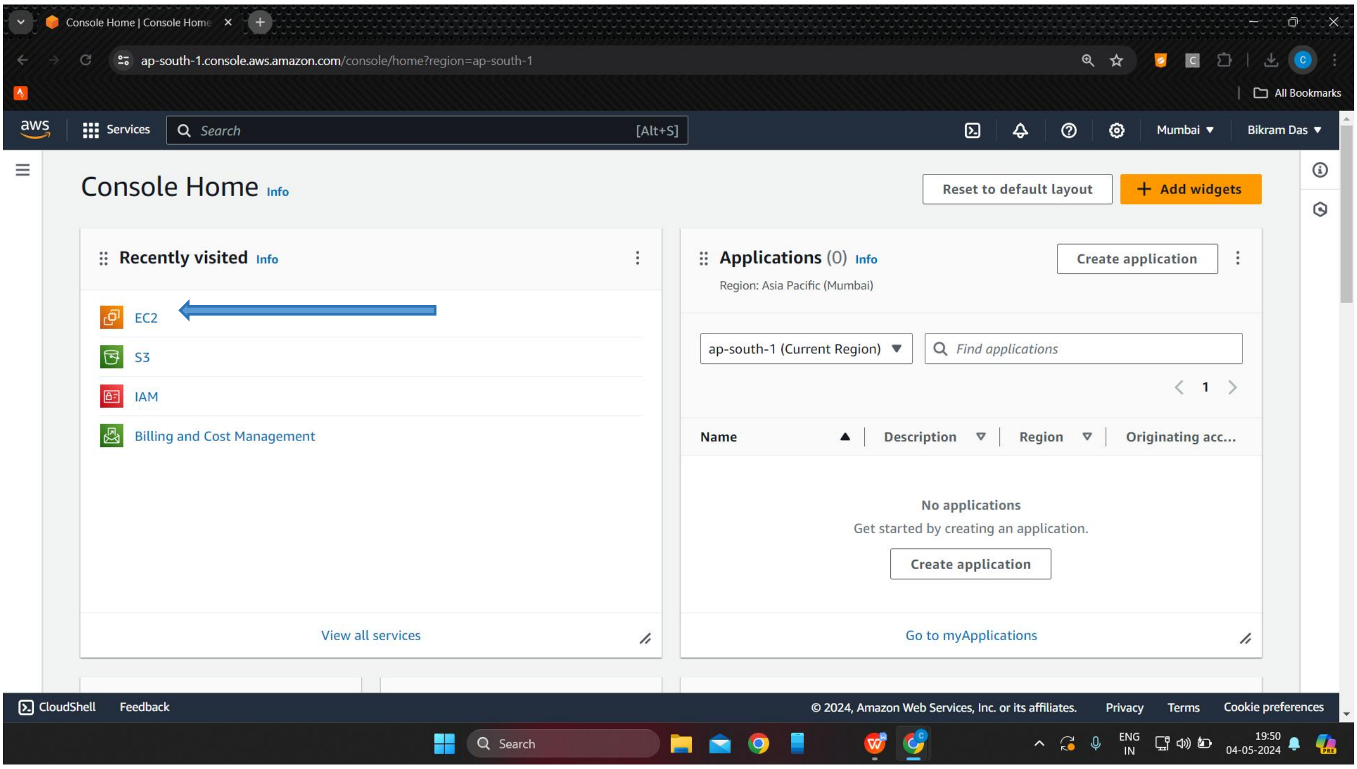
ASSIGNMENT 9

PROBLEM STATEMENT -> Deploy a project from GitHub to EC2.

- **To Deploy the project --->**

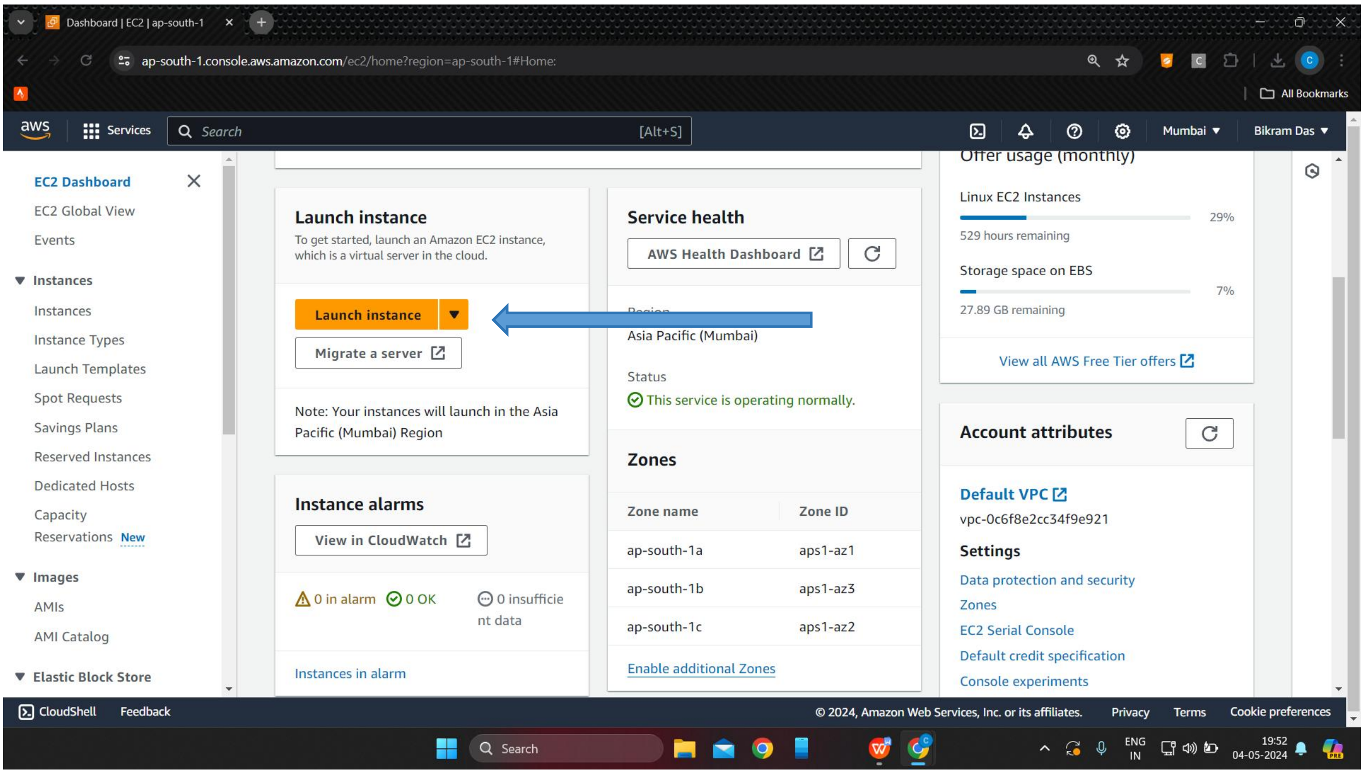
STEP 1-> Select EC2 option.



No applications

Get started by creating an application.

STEP 2-> Click on 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

Instance alarms

0 in alarm 0 OK 0 insufficient data

Service health

Region
Asia Pacific (Mumbai)

Status
This service is operating normally.

Zones

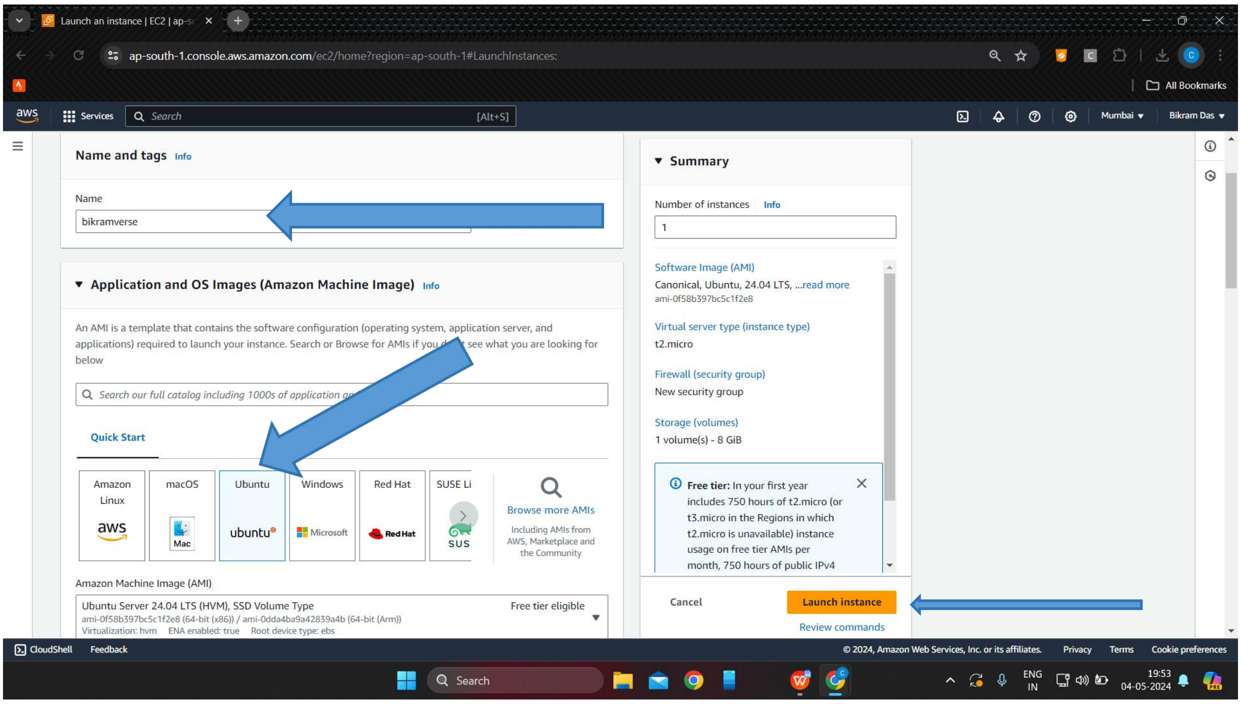
Zone name	Zone ID
ap-south-1a	aps1-az1
ap-south-1b	aps1-az3
ap-south-1c	aps1-az2

Linux EC2 Instances 29%
529 hours remaining

Storage space on EBS 7%
27.89 GB remaining

Default VPC
vpc-0c6f8e2cc34f9e921

STEP 3-> Give a unique name to the instance and select Ubuntu



Launch an instance | EC2 | ap-s

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

Name and tags Info

Name: bikramverse

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

Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Li
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0f58b397bc5c1f2e8 (64-bit (x86)) / ami-0dda4ba9a42839a4b (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0f58b397bc5c1f2e8

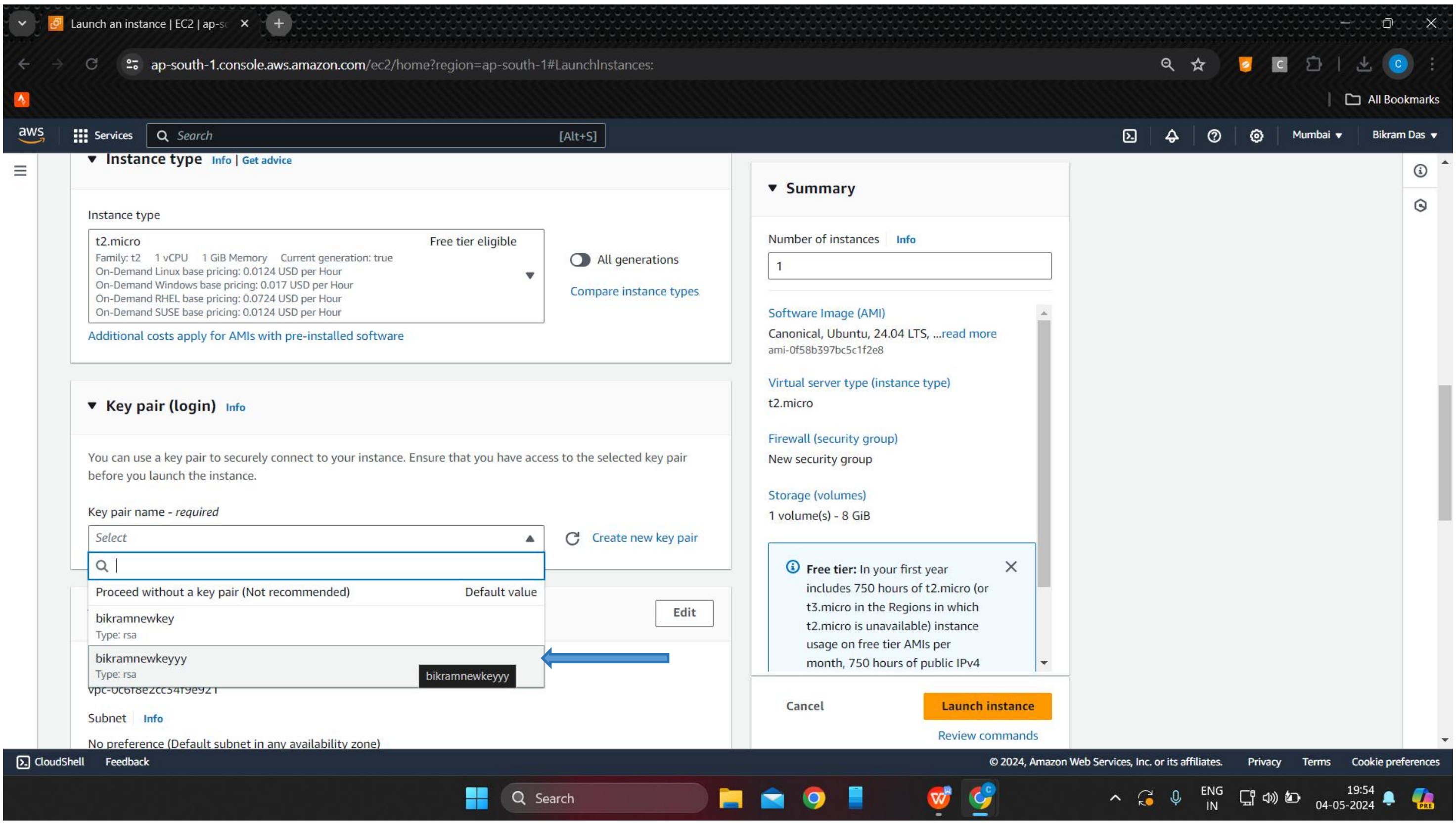
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4

STEP 4-> Select the key from the list or create a new one



Launch an instance | EC2 | ap-s

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

Instance type Info | Get advice

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0724 USD per Hour
On-Demand SUSE base pricing: 0.0124 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*

Select

Proceed without a key pair (Not recommended) — Default value
bikramnewkey
Type: rsa
bikramnewkeyyy
Type: rsa

Subnet Info

No preference (Default subnet in any availability zone)

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0f58b397bc5c1f2e8

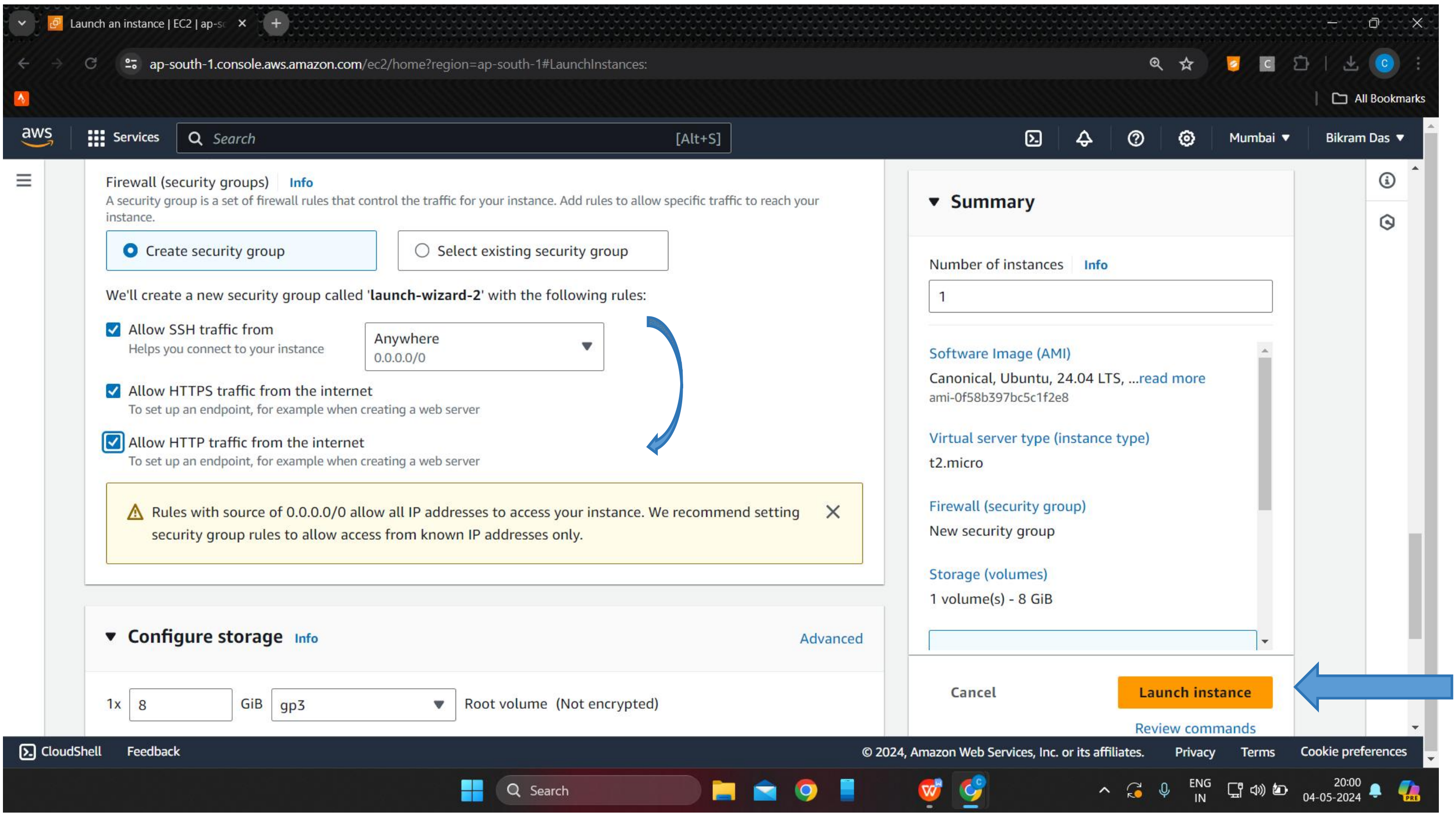
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4

STEP 5-> Check all the 3 check boxes under the Network Settings. Then click on Launch Instance.



Launch an instance | EC2 | ap-s

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

Services | Search [Alt+S] | Mumbai ▼ | Bikram Das ▼

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-2**' with the following rules:

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

☑ 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

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ **Configure storage** Info — Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

▼ **Summary**

Number of instances Info: 1

Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0f58b397bc5c1f2e8

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

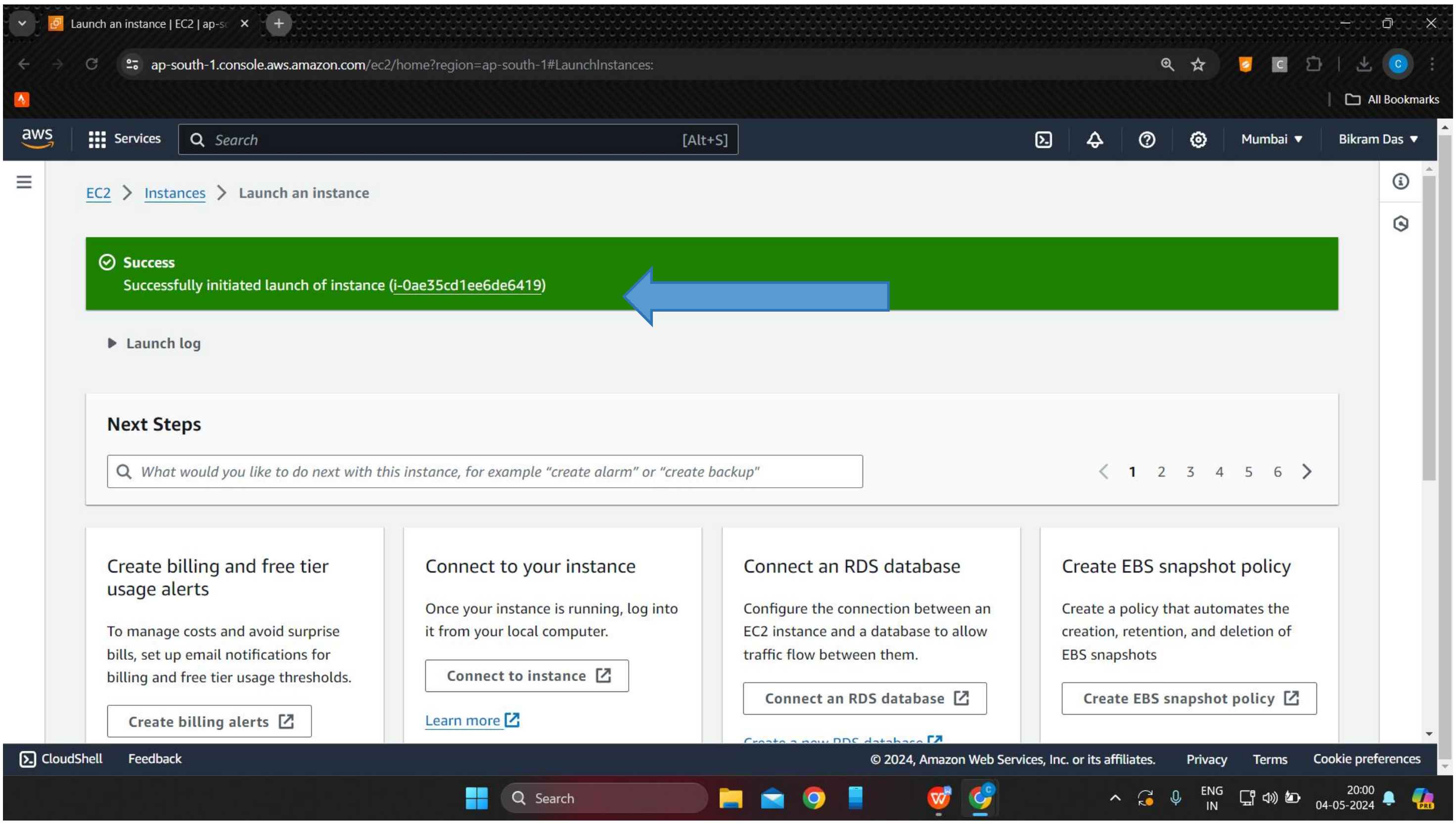
Cancel | Launch instance

Review commands

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

20:00 04-05-2024

STEP 6-> Click on instance id to enter into the instance.



Launch an instance | EC2 | ap-s

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

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0ae35cd1ee6de6419)

▶ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

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.
Create billing alerts

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

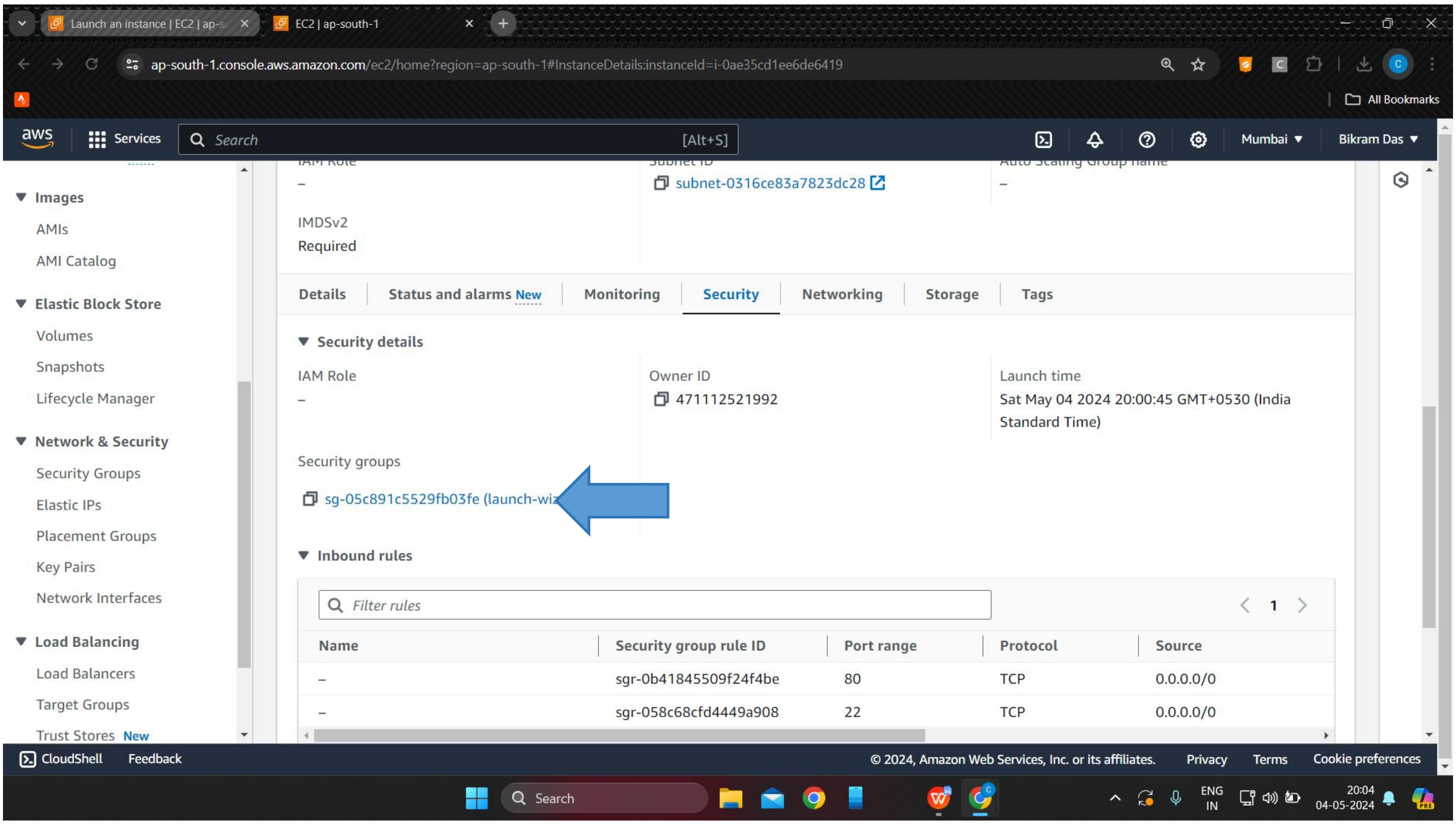
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

20:00 04-05-2024

STEP 7-> Select the Security option & Click on the security groupID.



IAM Role
–

Subnet ID
subnet-0316ce83a7823dc28

Auto Scaling Group name
–

IMDSv2
Required

Security details

IAM Role
–

Owner ID
471112521992

Launch time
Sat May 04 2024 20:00:45 GMT+0530 (India Standard Time)

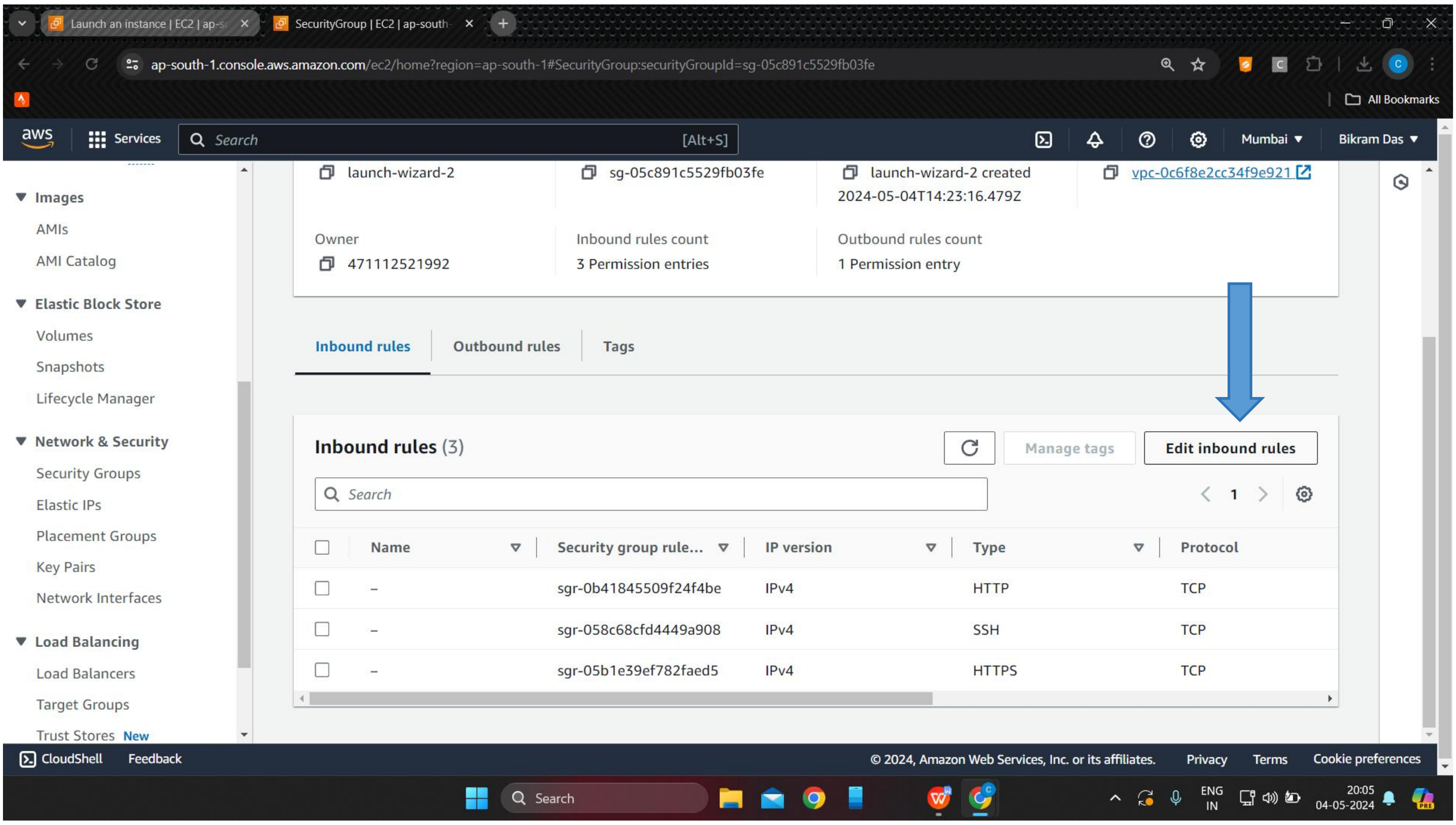
Security groups
sg-05c891c5529fb03fe (launch-wiz

Inbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Source
–	sgr-0b41845509f24f4be	80	TCP	0.0.0.0/0
–	sgr-058c68cfd4449a908	22	TCP	0.0.0.0/0

STEP 8->Click on Edit Inbound Rules



launch-wizard-2
sg-05c891c5529fb03fe
launch-wizard-2 created 2024-05-04T14:23:16.479Z
vpc-0c6f8e2cc34f9e921

Owner
471112521992

Inbound rules count
3 Permission entries

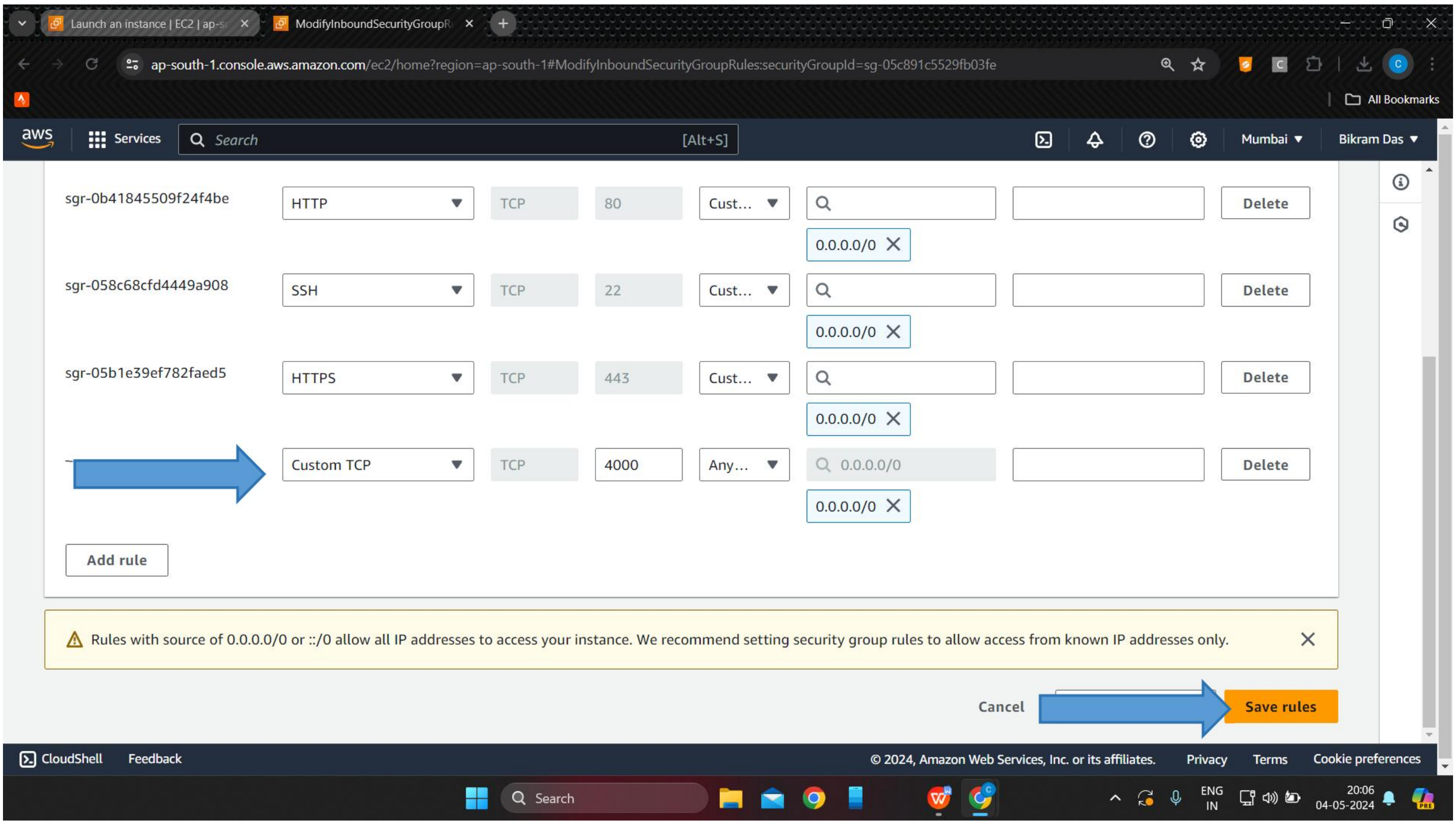
Outbound rules count
1 Permission entry

Inbound rules (3)

Search

□	Name	Security group rule...	IP version	Type	Protocol
□	–	sgr-0b41845509f24f4be	IPv4	HTTP	TCP
□	–	sgr-058c68cfd4449a908	IPv4	SSH	TCP
□	–	sgr-05b1e39ef782faed5	IPv4	HTTPS	TCP

STEP 9-> Click on Add Rules button after which give the port no. 4000, insource info give 0.0.0.0/0. Then click on Save Rules.



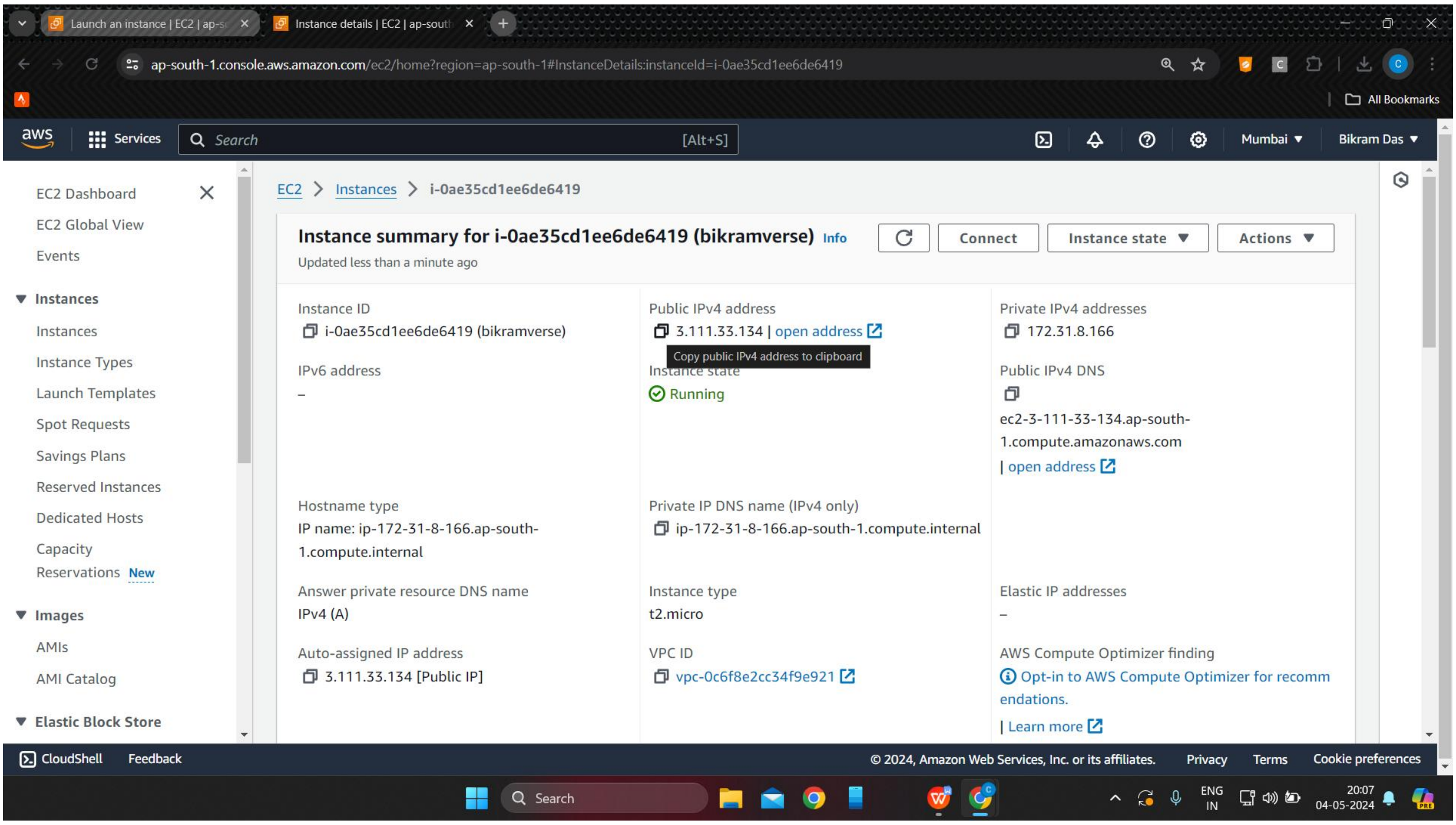
Launch an instance | EC2 | ap-s
ModifyInboundSecurityGroupR
ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ModifyInboundSecurityGroupRules:securityGroupId=sg-05c891c5529fb03fe
All Bookmarks
aws
Services
Search
[Alt+S]
Mumbai ▼
Bikram Das ▼

sgr-0b41845509f24f4be	HTTP ▼	TCP	80	Cust... ▼	0.0.0.0/0 ✕		Delete
sgr-058c68cfd4449a908	SSH ▼	TCP	22	Cust... ▼	0.0.0.0/0 ✕		Delete
sgr-05b1e39ef782faed5	HTTPS ▼	TCP	443	Cust... ▼	0.0.0.0/0 ✕		Delete
	Custom TCP ▼	TCP	4000	Any... ▼	0.0.0.0/0 0.0.0.0/0 ✕		Delete

Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

STEP 10-> Go back into the instance and copy the Public IPv4 Address.

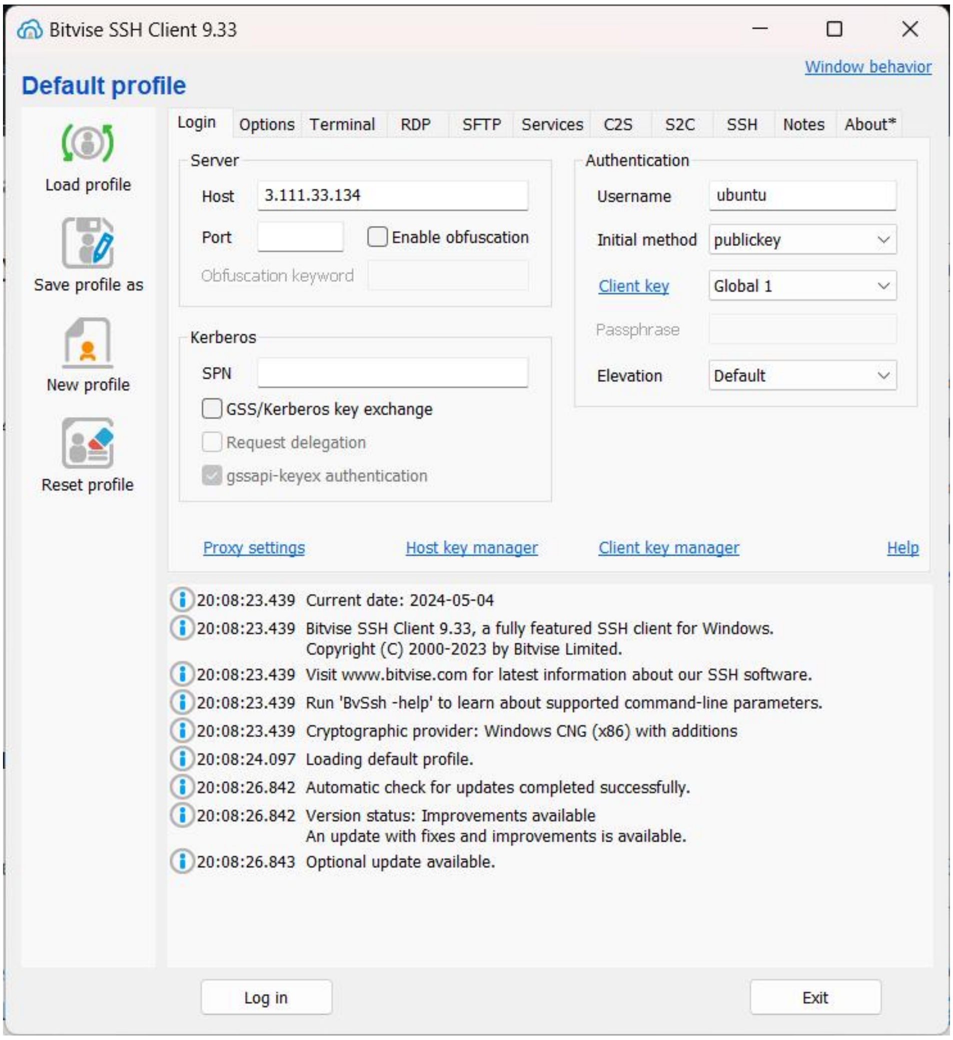


Instance summary for i-0ae35cd1ee6de6419 (bikramverse) Info

Updated less than a minute ago

Instance ID i-0ae35cd1ee6de6419 (bikramverse)	Public IPv4 address 3.111.33.134 | open address Copy public IPv4 address to clipboard	Private IPv4 addresses 172.31.8.166
IPv6 address –	Instance state Running	Public IPv4 DNS ec2-3-111-33-134.ap-south-1.compute.amazonaws.com | open address
Hostname type IP name: ip-172-31-8-166.ap-south-1.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-8-166.ap-south-1.compute.internal	
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address 3.111.33.134 [Public IP]	VPC ID vpc-0c6f8e2cc34f9e921	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more

STEP 11-> Paste the address under the host tab. Under the Authenticationtab, give the username as ubuntu, Initial method as publickey. Then clickonClientKey Manager.



Server

Host: 3.111.33.134

Port:

□ Enable obfuscation

Obfuscation keyword:

Kerberos

SPN:

□ GSS/Kerberos key exchange

□ Request delegation

☑ gssapi-keyex authentication

Authentication

Username: ubuntu

Initial method: publickey

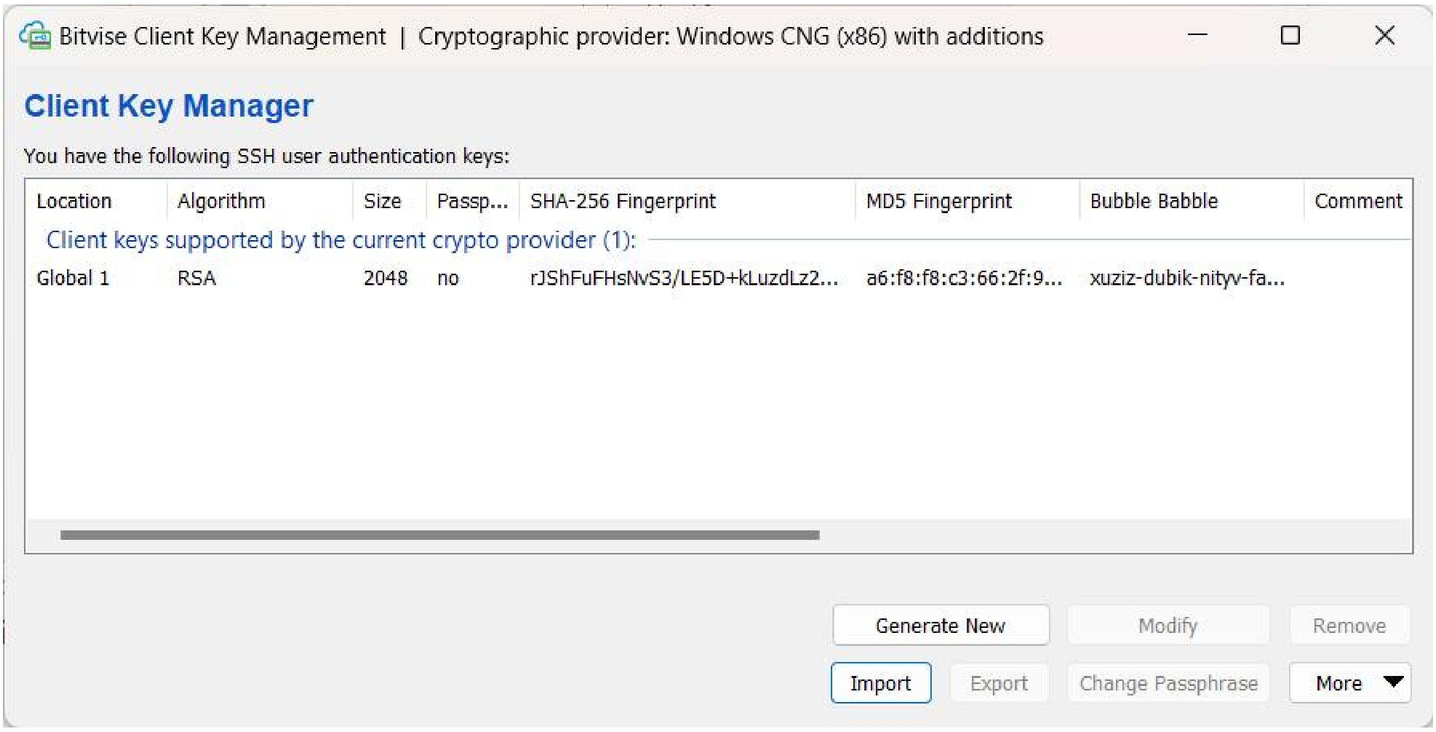
Client key: Global 1

Passphrase:

Elevation: Default

```
20:08:23.439  Current date: 2024-05-04
20:08:23.439  Bitvise SSH Client 9.33, a fully featured SSH client for Windows.
              Copyright (C) 2000-2023 by Bitvise Limited.
20:08:23.439  Visit www.bitvise.com for latest information about our SSH software.
20:08:23.439  Run 'BvSsh -help' to learn about supported command-line parameters.
20:08:23.439  Cryptographic provider: Windows CNG (x86) with additions
20:08:24.097  Loading default profile.
20:08:26.842  Automatic check for updates completed successfully.
20:08:26.842  Version status: Improvements available
              An update with fixes and improvements is available.
20:08:26.843  Optional update available.
```

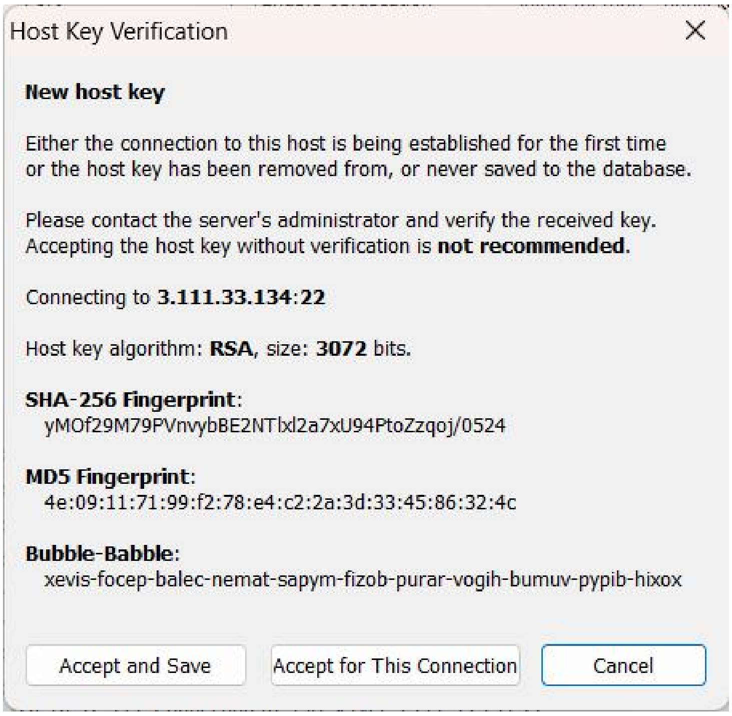
STEP 12-> Remove any previously selected key if any, the click onImport. Select the key using which instance was created. Then close the window.


Bitvise Client Key Management | Cryptographic provider: Windows CNG (x86) with additions
Client Key Manager
Generate New
Modify
Remove
Import
Export
Change Passphrase
More

You have the following SSH user authentication keys:

Location	Algorithm	Size	Passp...	SHA-256 Fingerprint	MD5 Fingerprint	Bubble Babble	Comment
Client keys supported by the current crypto provider (1):							
Global 1	RSA	2048	no	rJShFuFHsNvS3/LE5D+kLuzdLz2...	a6:f8:f8:c3:66:2f:9...	xuziz-dubik-nityv-fa...	

STEP 13-> Click on Login after that in host key verification click accept and save.



Host Key Verification

New host key

Either the connection to this host is being established for the first time
or the host key has been removed from, or never saved to the database.

Please contact the server's administrator and verify the received key.
Accepting the host key without verification is **not recommended**.

Connecting to **3.111.33.134:22**

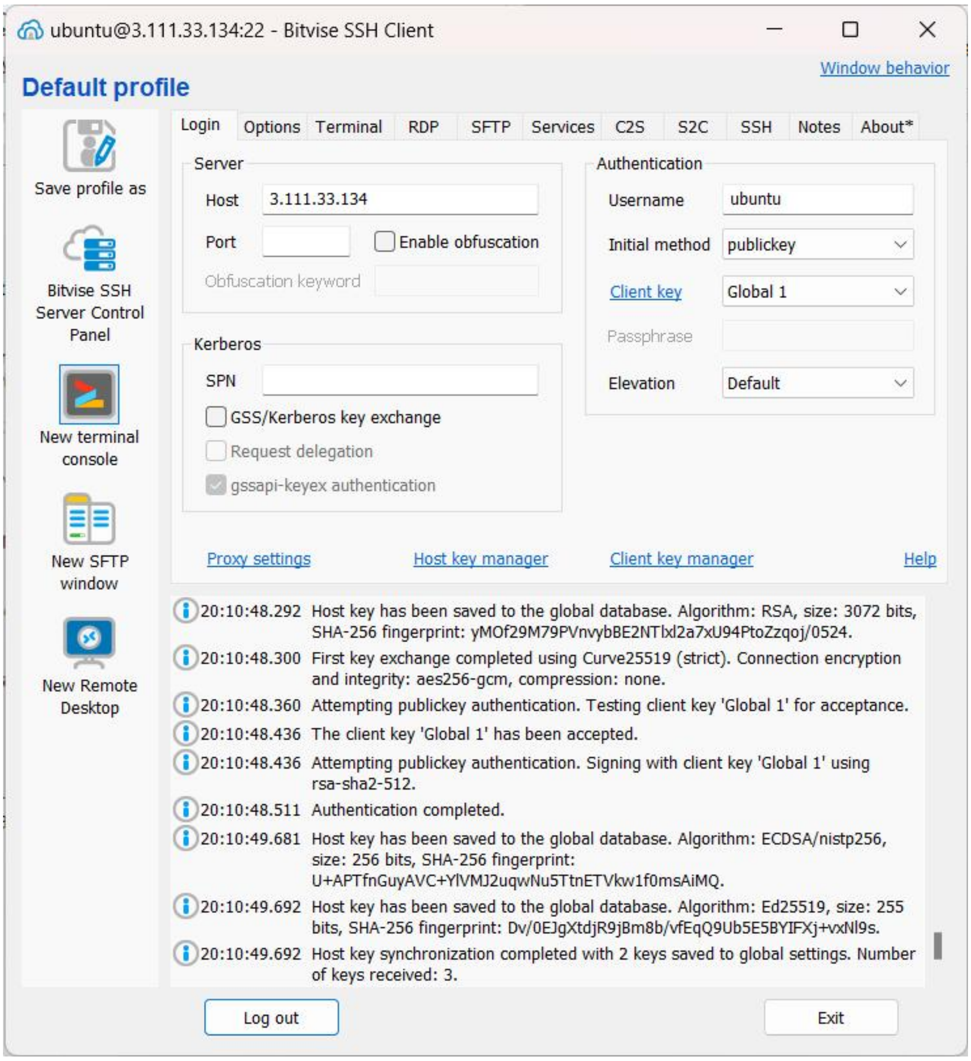
Host key algorithm: **RSA**, size: **3072** bits.

SHA-256 Fingerprint:
yMOf29M79PVnvybBE2NTlxl2a7xU94PtoZzqoj/0524

MD5 Fingerprint:
4e:09:11:71:99:f2:78:e4:c2:2a:3d:33:45:86:32:4c

Bubble-Babble:
xevis-focep-balec-nemat-sapym-fizob-purar-vogih-bumuv-pypib-hixox

STEP 14-> Open a new terminal by clicking on New Terminal Console.



ubuntu@3.111.33.134:22 - Bitvise SSH Client

Default profile

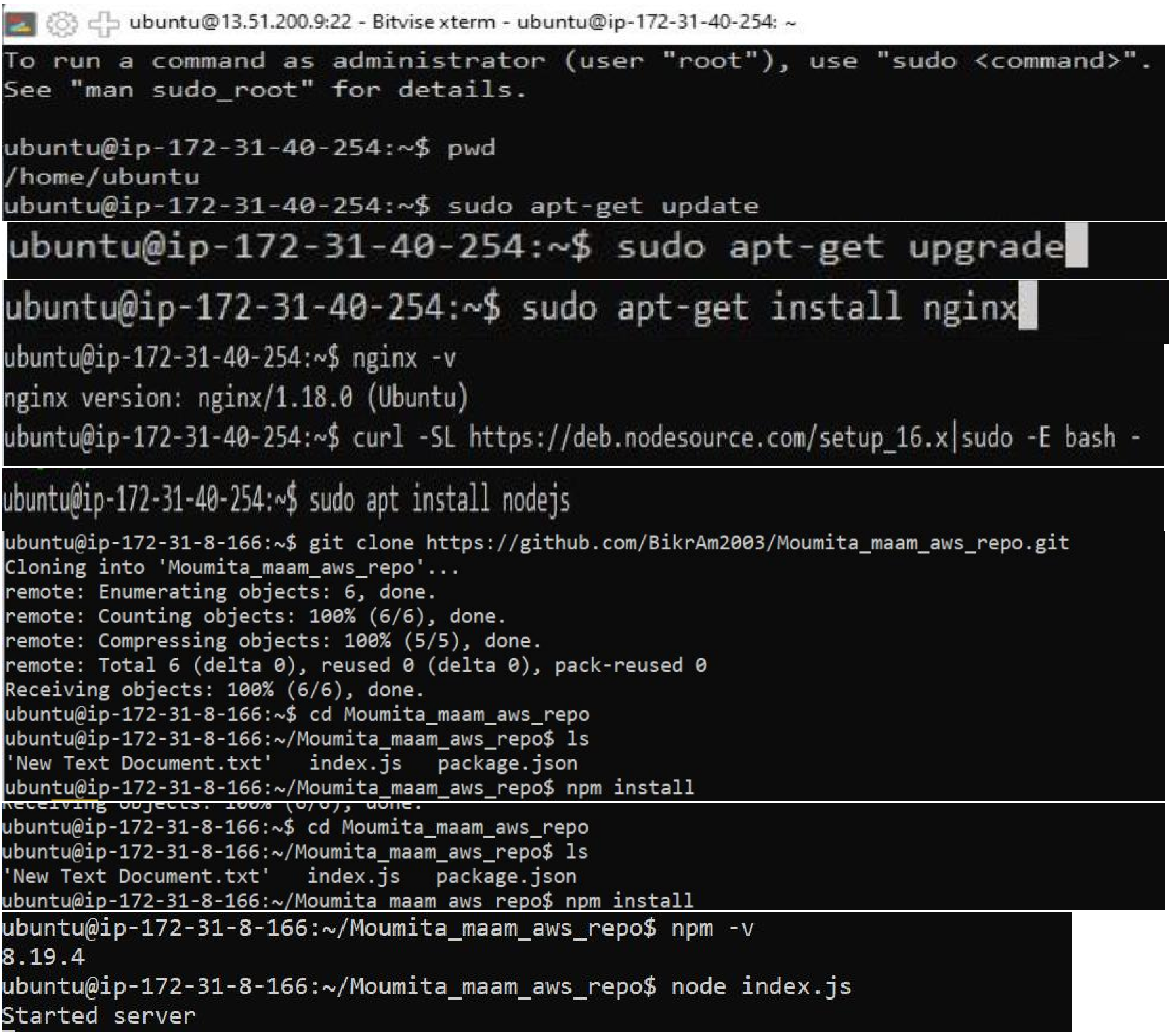
Server
Host: 3.111.33.134
Port:
□ Enable obfuscation
Obfuscation keyword:

Kerberos
SPN:
□ GSS/Kerberos key exchange
□ Request delegation
☑ gssapi-keyex authentication

Authentication
Username: ubuntu
Initial method: publickey
Client key: Global 1
Passphrase:
Elevation: Default

```
20:10:48.292 Host key has been saved to the global database. Algorithm: RSA, size: 3072 bits,
             SHA-256 fingerprint: yMOf29M79PVnvybBE2NTlxl2a7xU94PtoZzqoj/0524.
20:10:48.300 First key exchange completed using Curve25519 (strict). Connection encryption
             and integrity: aes256-gcm, compression: none.
20:10:48.360 Attempting publickey authentication. Testing client key 'Global 1' for acceptance.
20:10:48.436 The client key 'Global 1' has been accepted.
20:10:48.436 Attempting publickey authentication. Signing with client key 'Global 1' using
             rsa-sha2-512.
20:10:48.511 Authentication completed.
20:10:49.681 Host key has been saved to the global database. Algorithm: ECDSA/nistp256,
             size: 256 bits, SHA-256 fingerprint:
             U+APTfnGuyAVC+YlVMJ2uqwNu5TtnETVkw1f0msAiMQ.
20:10:49.692 Host key has been saved to the global database. Algorithm: Ed25519, size: 255
             bits, SHA-256 fingerprint: Dv/0EJgXtdjR9jBm8b/vfEqQ9Ub5E5BYIFXj+vxNl9s.
20:10:49.692 Host key synchronization completed with 2 keys saved to global settings. Number
             of keys received: 3.
```

STEP 15-> In the console type the following commands in sequential order:

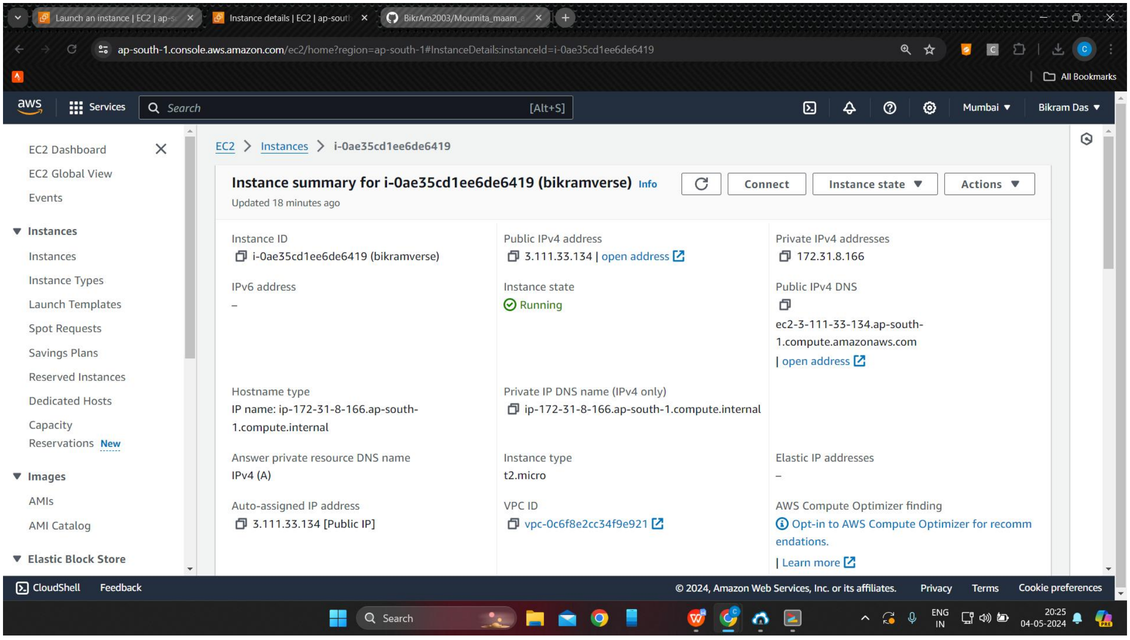


ubuntu@13.51.200.9:22 - Bitvise xterm - ubuntu@ip-172-31-40-254: ~

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-40-254:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-40-254:~$ sudo apt-get update
ubuntu@ip-172-31-40-254:~$ sudo apt-get upgrade
ubuntu@ip-172-31-40-254:~$ sudo apt-get install nginx
ubuntu@ip-172-31-40-254:~$ nginx -v
nginx version: nginx/1.18.0 (Ubuntu)
ubuntu@ip-172-31-40-254:~$ curl -SL https://deb.nodesource.com/setup_16.x|sudo -E bash -
ubuntu@ip-172-31-40-254:~$ sudo apt install nodejs
ubuntu@ip-172-31-8-166:~$ git clone https://github.com/BikrAm2003/Moumita_maam_aws_repo.git
Cloning into 'Moumita_maam_aws_repo'...
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 6 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (6/6), done.
ubuntu@ip-172-31-8-166:~$ cd Moumita_maam_aws_repo
ubuntu@ip-172-31-8-166:~/Moumita_maam_aws_repo$ ls
'New Text Document.txt'   index.js   package.json
ubuntu@ip-172-31-8-166:~/Moumita_maam_aws_repo$ npm install
Receiving objects: 100% (6/6), done.
ubuntu@ip-172-31-8-166:~$ cd Moumita_maam_aws_repo
ubuntu@ip-172-31-8-166:~/Moumita_maam_aws_repo$ ls
'New Text Document.txt'   index.js   package.json
ubuntu@ip-172-31-8-166:~/Moumita_maam_aws_repo$ npm install
ubuntu@ip-172-31-8-166:~/Moumita_maam_aws_repo$ npm -v
8.19.4
ubuntu@ip-172-31-8-166:~/Moumita_maam_aws_repo$ node index.js
Started server
```

STEP 16-> From the Public IPv4 Address copy the Address and Paste it on a new tab.



Instance summary for i-0ae35cd1ee6de6419 (bikramverse) Info

Updated 18 minutes ago

Instance ID
i-0ae35cd1ee6de6419 (bikramverse)

Public IPv4 address
3.111.33.134 | open address

Private IPv4 addresses
172.31.8.166

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-3-111-33-134.ap-south-1.compute.amazonaws.com | open address

Hostname type
IP name: ip-172-31-8-166.ap-south-1.compute.internal

Private IP DNS name (IPv4 only)
ip-172-31-8-166.ap-south-1.compute.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.micro

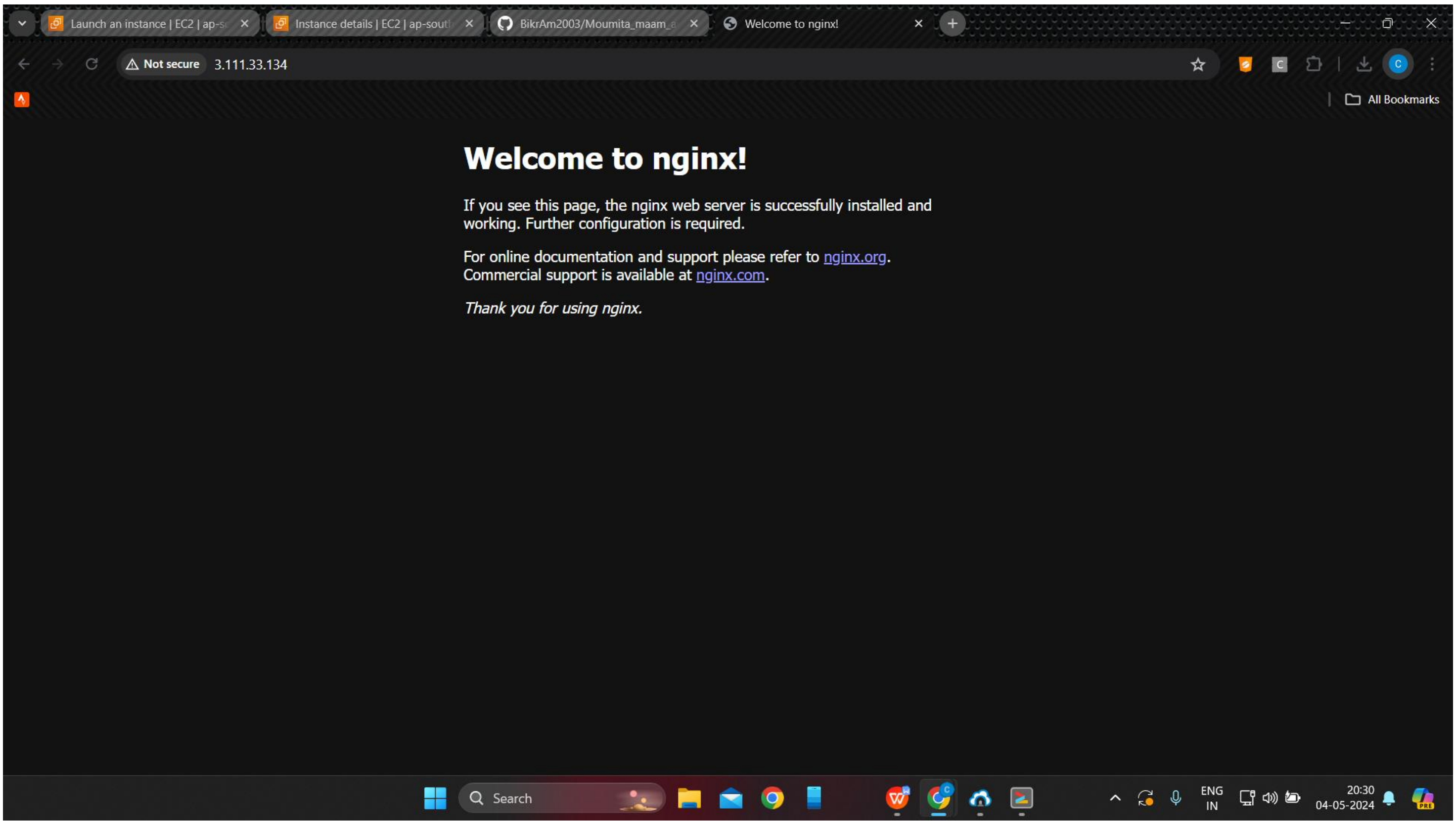
Elastic IP addresses
–

Auto-assigned IP address
3.111.33.134 [Public IP]

VPC ID
vpc-0c6f8e2cc34f9e921

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more

STEP 17-> Nginx window will open. Now add :4000 at the end of the IPv4Address.



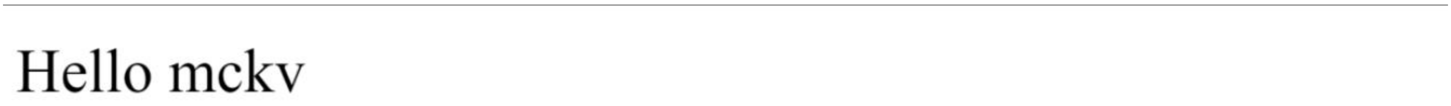
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

STEP 18-> The Nodejs file content will be visible.



Hello mckv