



PROJECT 3 >>

GRAFANA

INTEGRATING GRAFANA WITH LINUX SERVER

PRESENTED BY AMOD PATHAK >>



INTRODUCTION

Here we will try to learn about integration of grafana with linux server for high cpu utilization and create a graph in grafana

WHAT IS GRAFANA?

Grafana is an open-source platform for data visualization and analytics. It allows you to collect data from various sources, analyze it, and create informative dashboards to monitor your systems and applications

STEPS TO INTEGRATE GRAFANA WITH LINUX:-

1. Sign in to AWS console
2. Create an EC2 instance
3. Connecting public Ip with putty
4. Running given commands on putty
5. Open AWS console and create Policy and role
6. Enter grafana and create graph

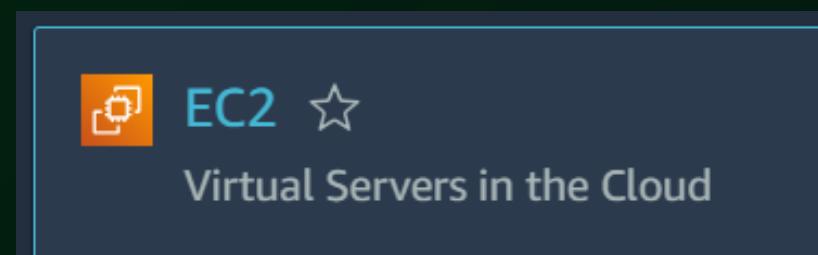
STEP -1

Sign in to AWS console

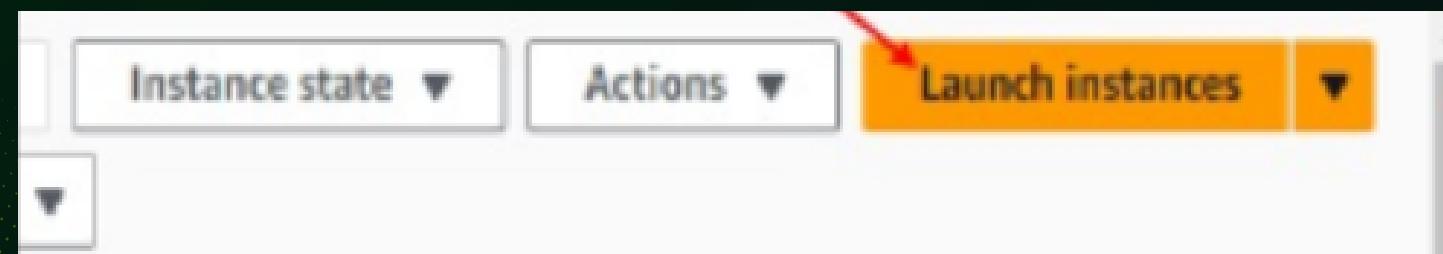
- Sign in to the AWS console using your root id and password
- Select region Asia Pacific(Mumbai) ap-south-1

STEP -2

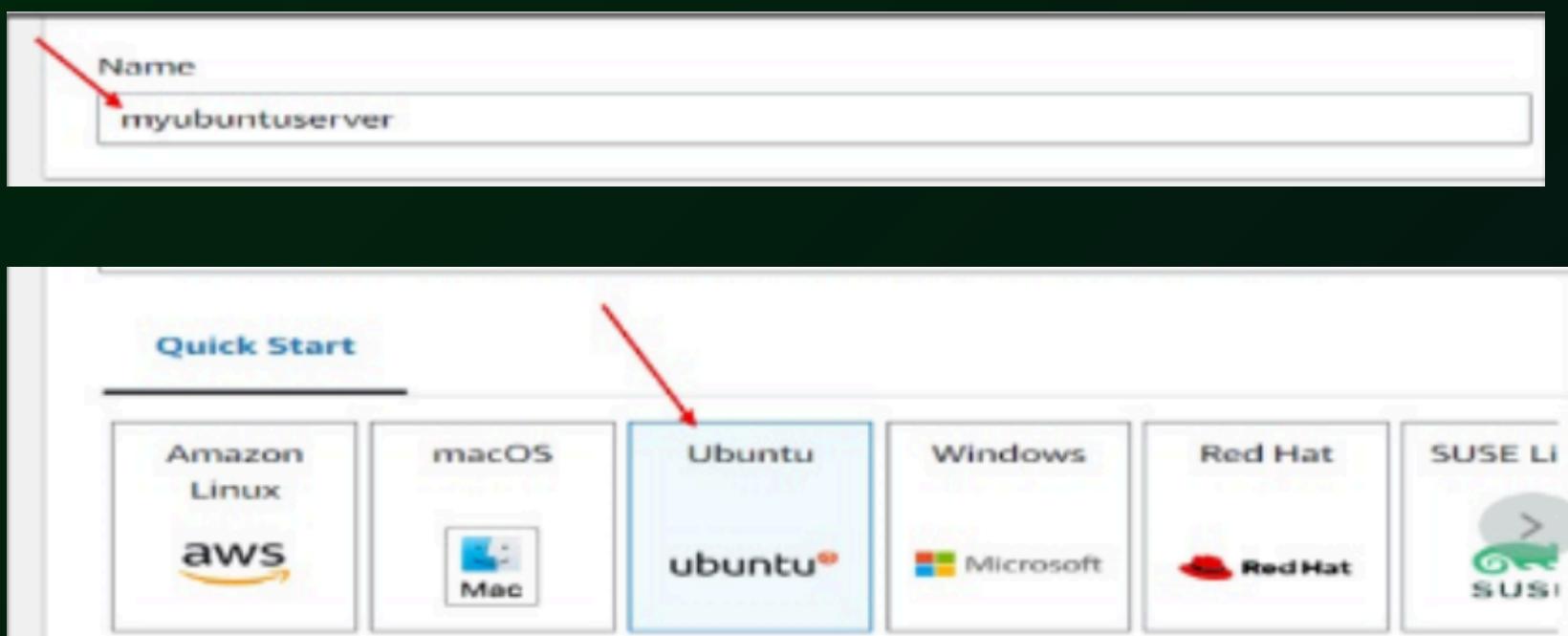
Create an EC2 instance



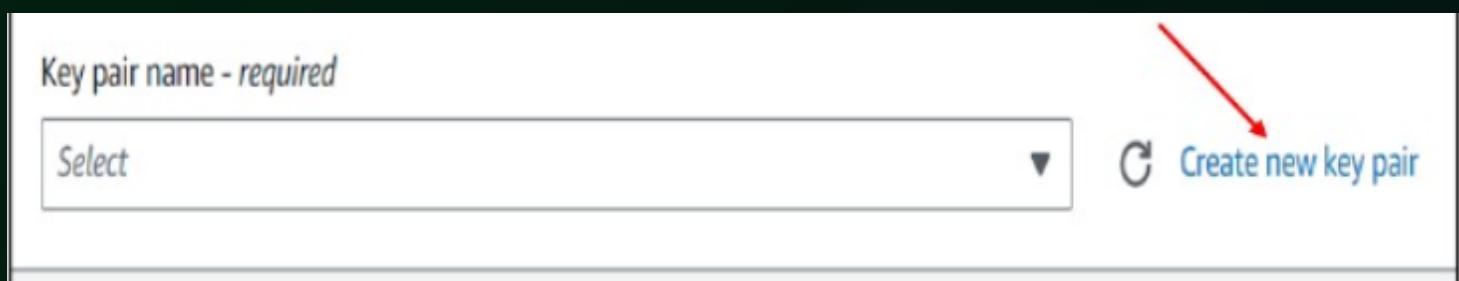
- Select EC2 and click on launch an instance



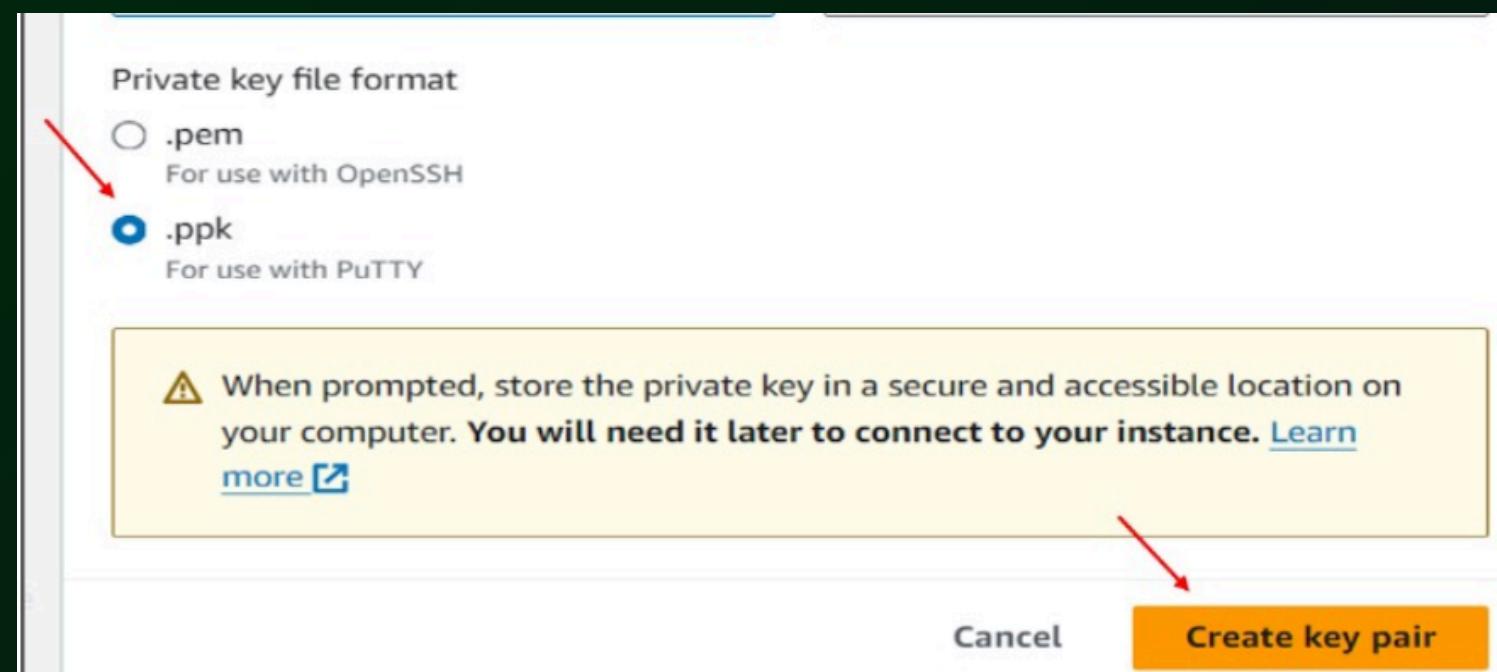
- Enter an instance name and select ubuntu as OS images(AMI)



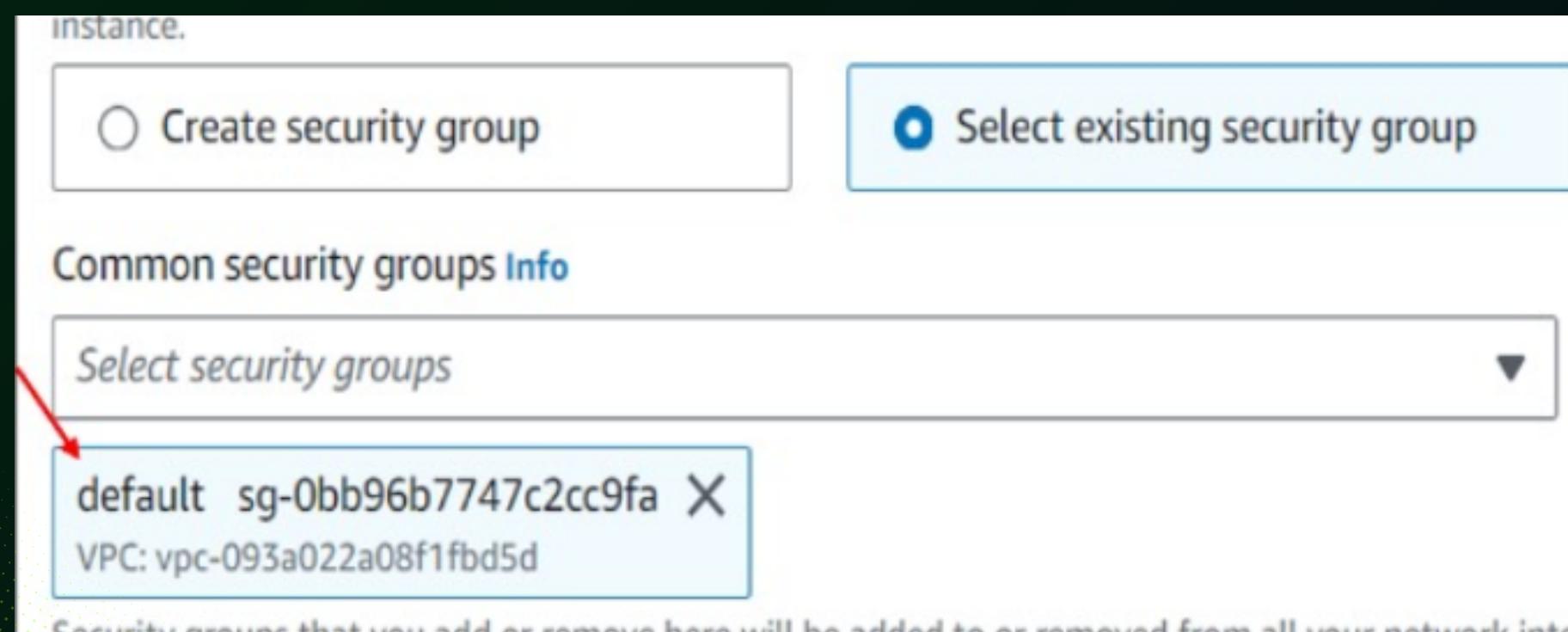
- Now select “create new key pair”

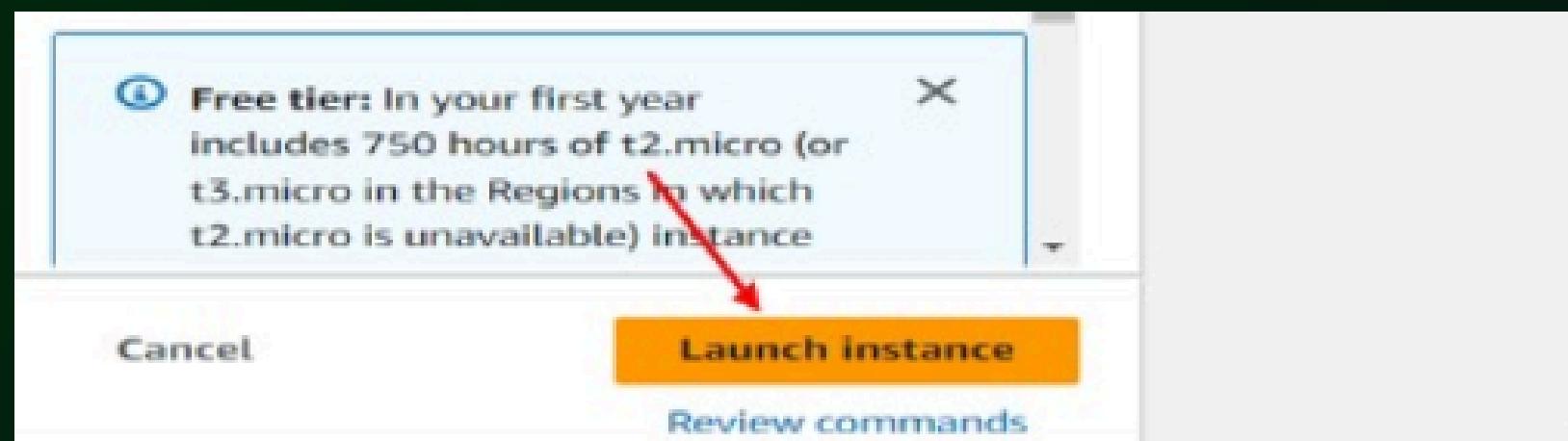


- Enter key pair name and select .ppk
- Click on create key pair



- Then select existing security group and select default
- Now click on “launch instance”

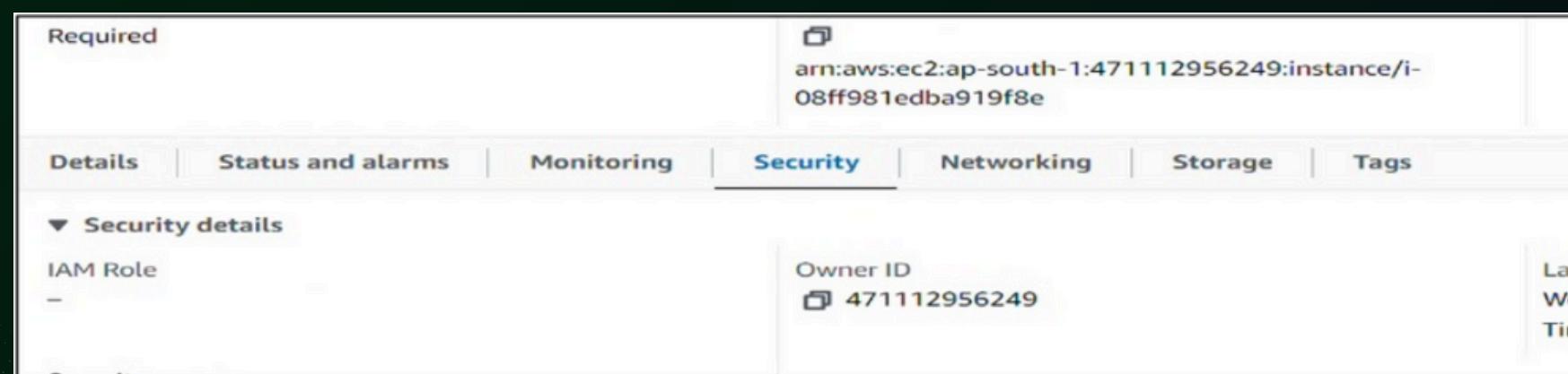




- Now your instance has been launched

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
myubuntuserver	i-0917f696f01331946	Pending	t2.micro	-	View alarms +	ap-south-1a	ec2-3-110-

- Now open your instance and go to security



- Go to inbound rules and click on default

Inbound rules					
<input type="text"/> Filter rules					
Security group rule ID	Port range	Protocol	Source	Security groups	Description
sgr-0c84cb7504a90d585	All	All	0.0.0.0/0	default	-

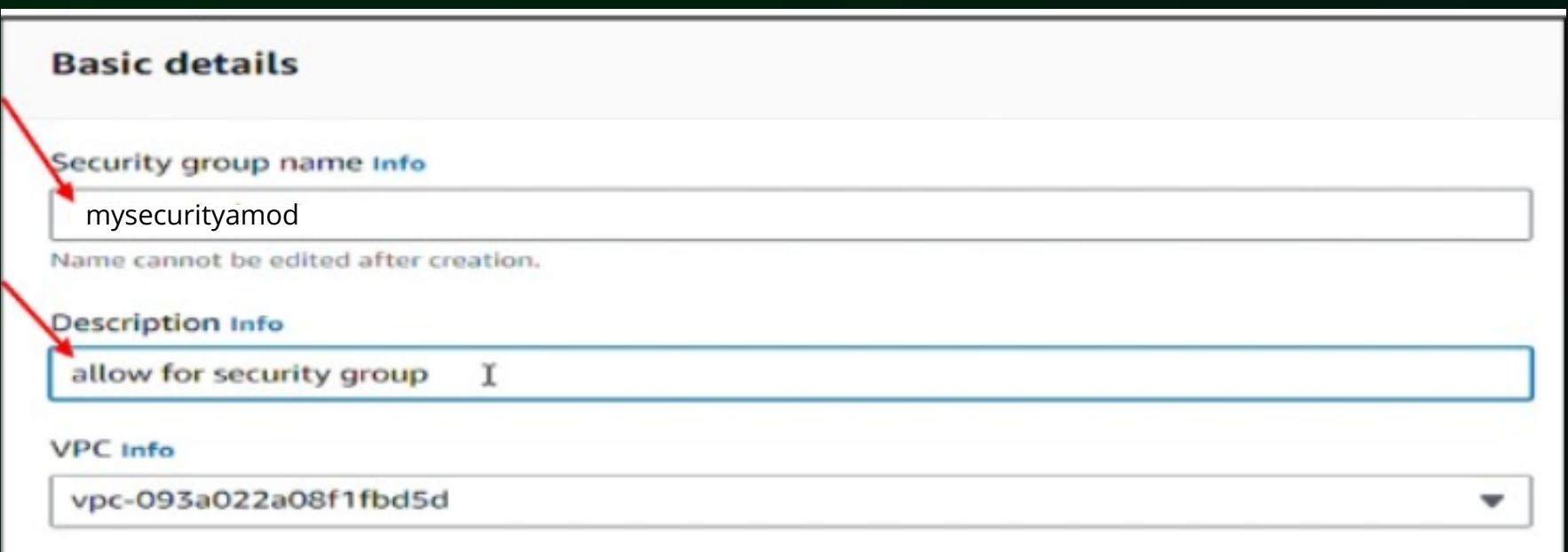
- Then click on security group and click add rule

The first screenshot shows the 'Inbound rules' section of the AWS Lambda console. A red arrow points to the 'Create security group' button, which is highlighted in orange. The second screenshot shows the 'Inbound rules Info' page for a new security group. It displays the message 'This security group has no inbound rules.' and features a prominent 'Add rule' button.

- In type info select all traffic and in source info select "anywhere-Ipv4"

The screenshot shows the 'Inbound rules Info' page for a security group. It includes fields for 'Type Info' (set to 'All traffic'), 'Protocol Info' (set to 'All'), 'Port range Info' (set to 'All'), and 'Source Info'. The 'Source Info' dropdown is open, showing options: 'Custom' (selected), 'Anywhere-IPv4' (highlighted with a red arrow), 'Anywhere-IPv6', and 'My IP'.

- Then click create security group
- Enter your security group name
- Then allow for security group in description

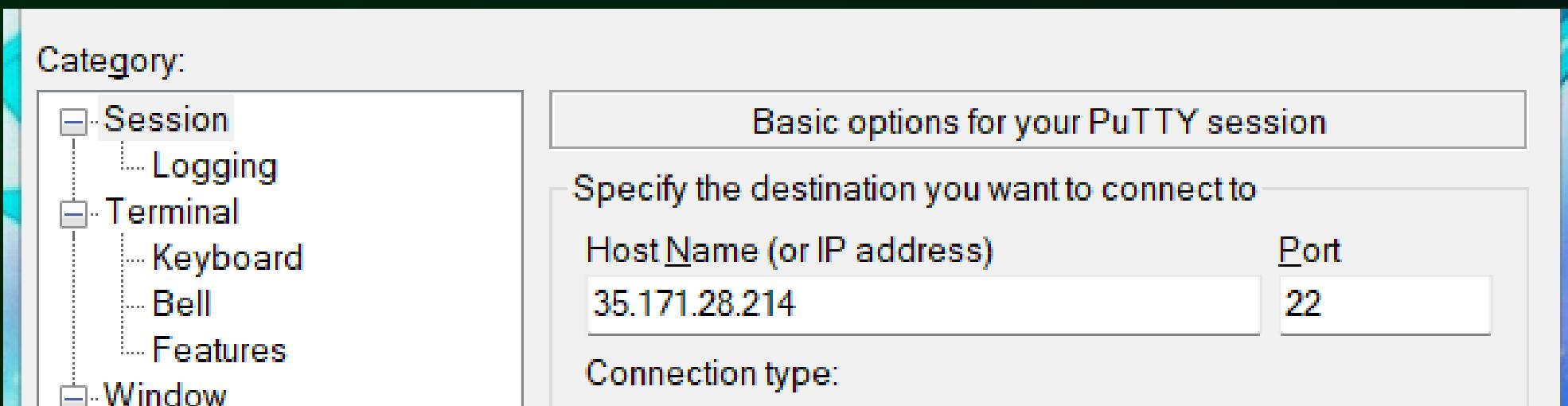


STEP -3

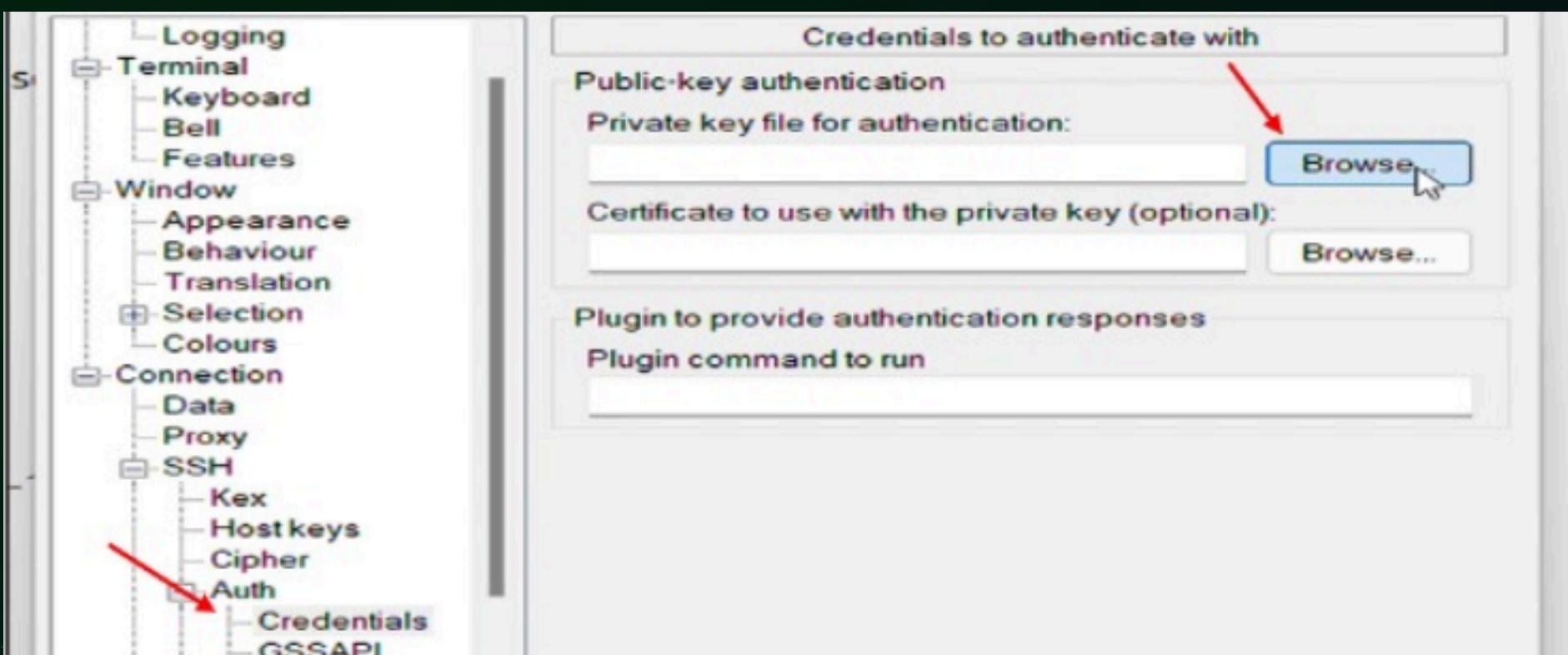
Connecting public Ip with putty

- Open putty and enter your public ip





- Now go to SSH and Enter Auth and tap on credentials
- Click on browse and Select your created key pair and open it

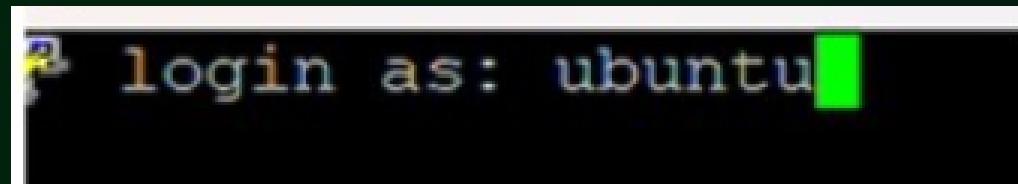




STEP -4

Running given commands on putty

- Login as ubuntu in putty server



- Enter the commands given below one by one respectively

```
sudo apt update
```

```
$ wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -
```

```
$ sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
```

```
$ sudo apt update
```

```
$ apt-cache policy grafana
```

```
$ sudo apt install grafana
```

```
$ sudo systemctl start grafana-server
```

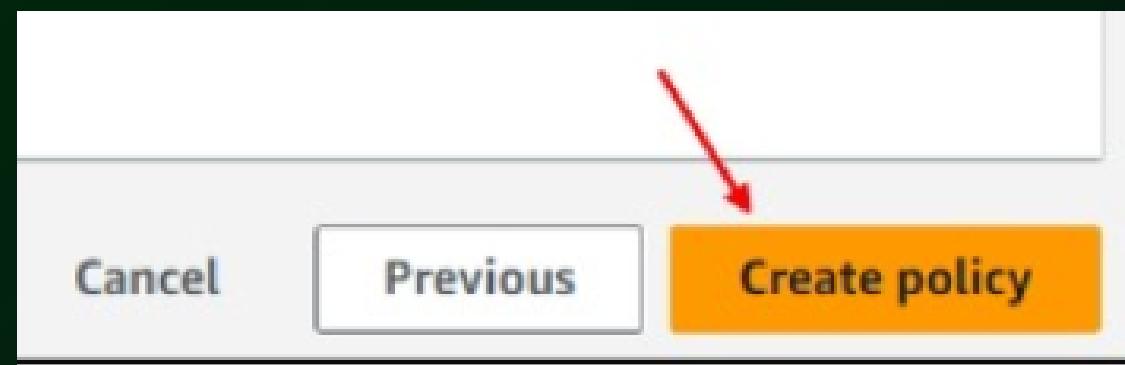
```
$ sudo systemctl status grafana-server
```

```
$ sudo systemctl enable grafana-server
```

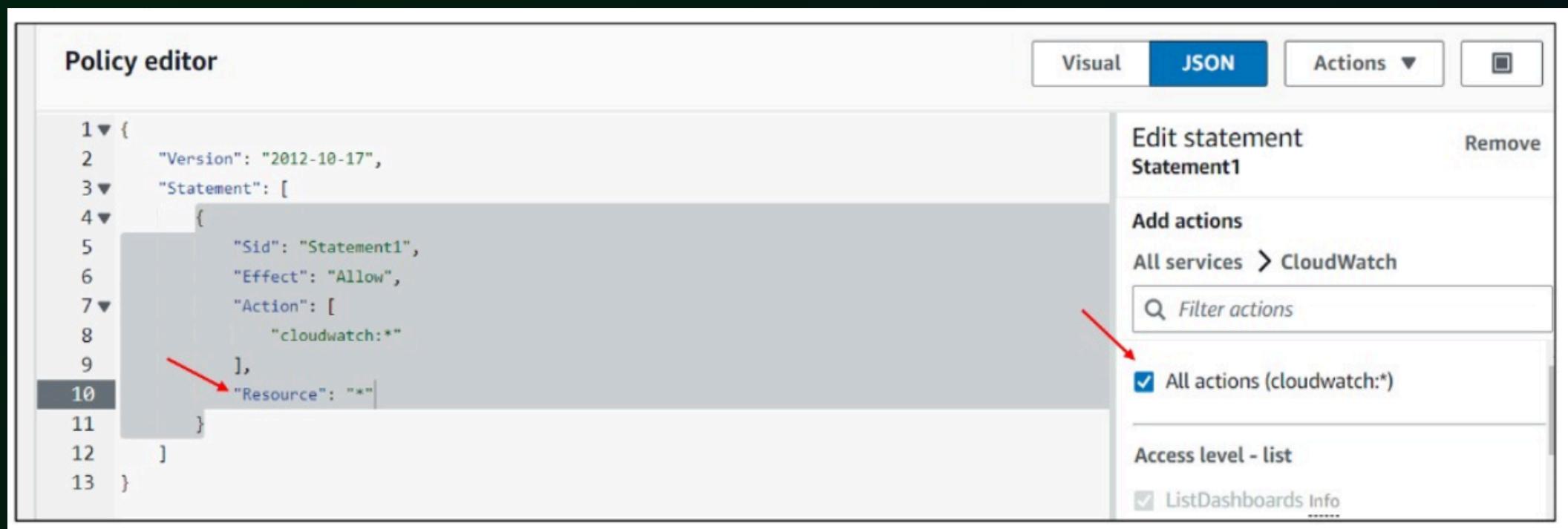
STEP -5

Opening AWS console and creating policy and role

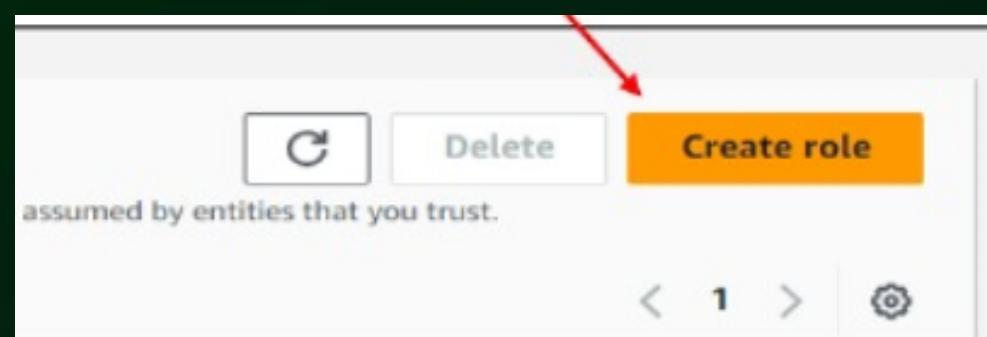
- Now first we have to go to Services and open IAM
- Select policy tab and click on create policy



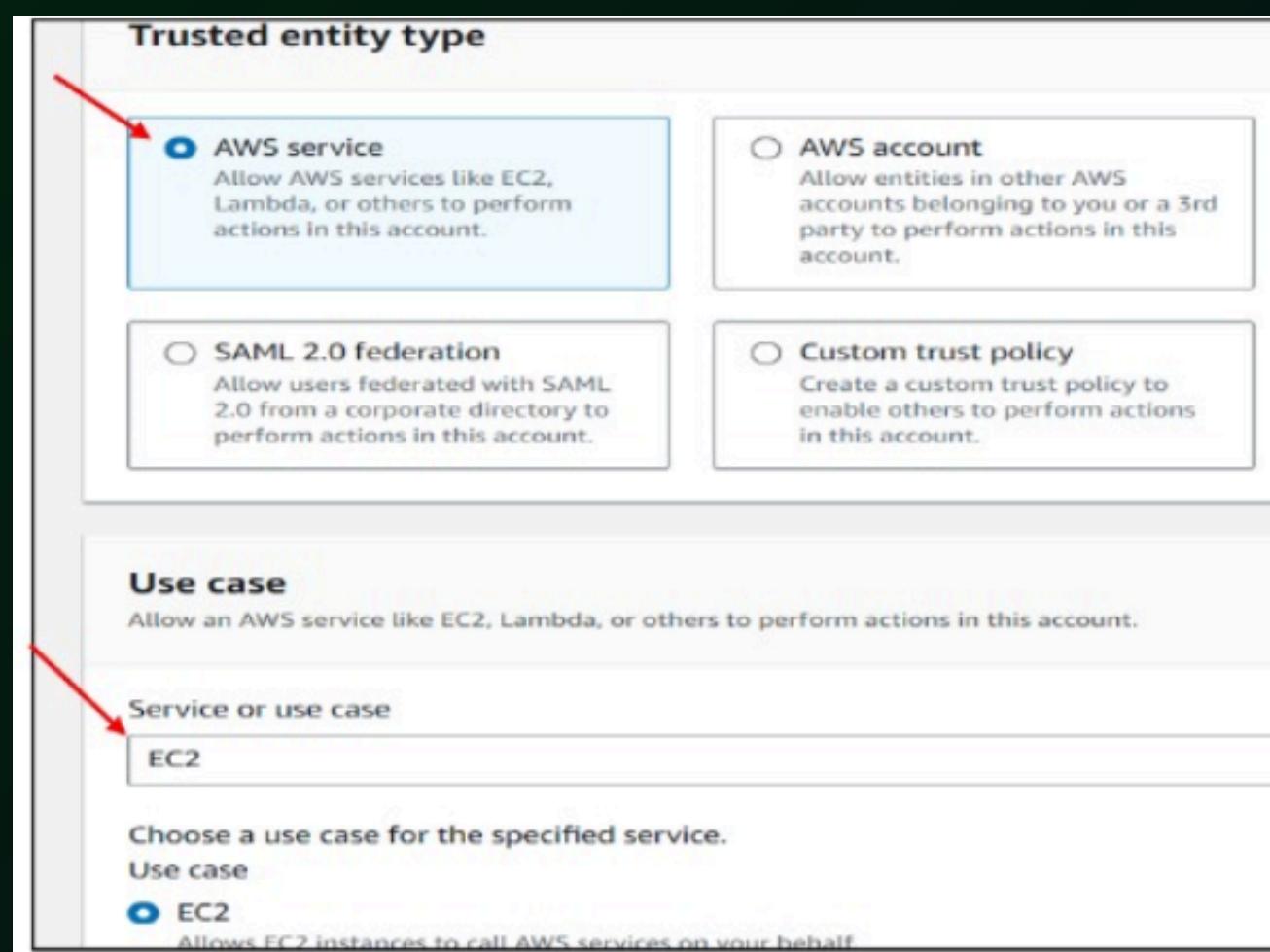
- Click on JSON and tap on “All actions (cloudwatch)”
- Then put resource “Resource:”“*”
- Now click on create policy (check attached docs for help)



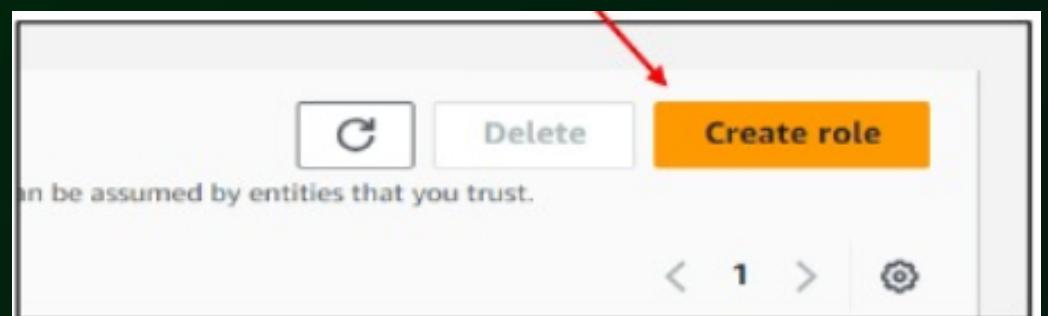
- Now go to roles and click on “create roles”



- Click on AWS service in “trusted entity type’ and use EC2 in use case
- Click on Next

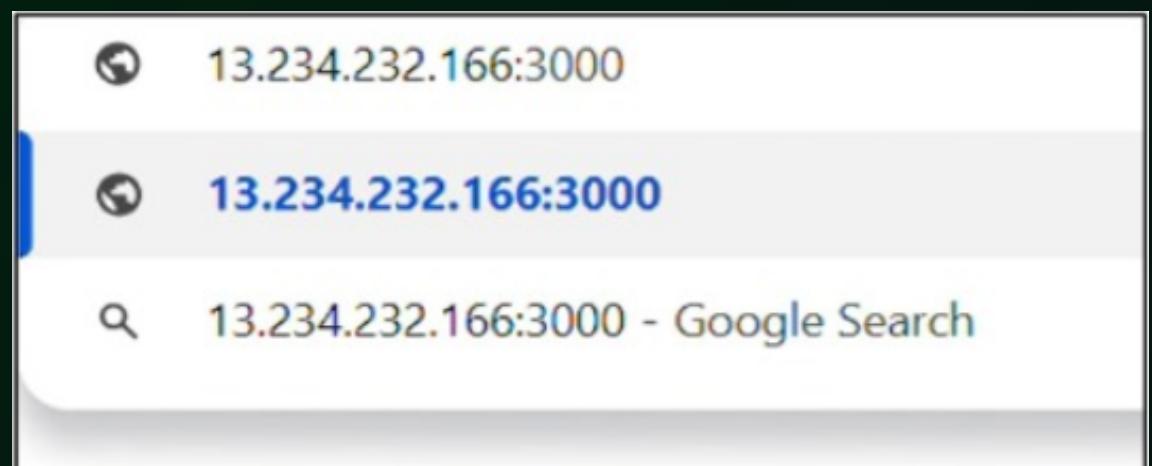


- Now enter your role name and click on CREATE ROLE



STEP-6 Enter Grafana and create graph

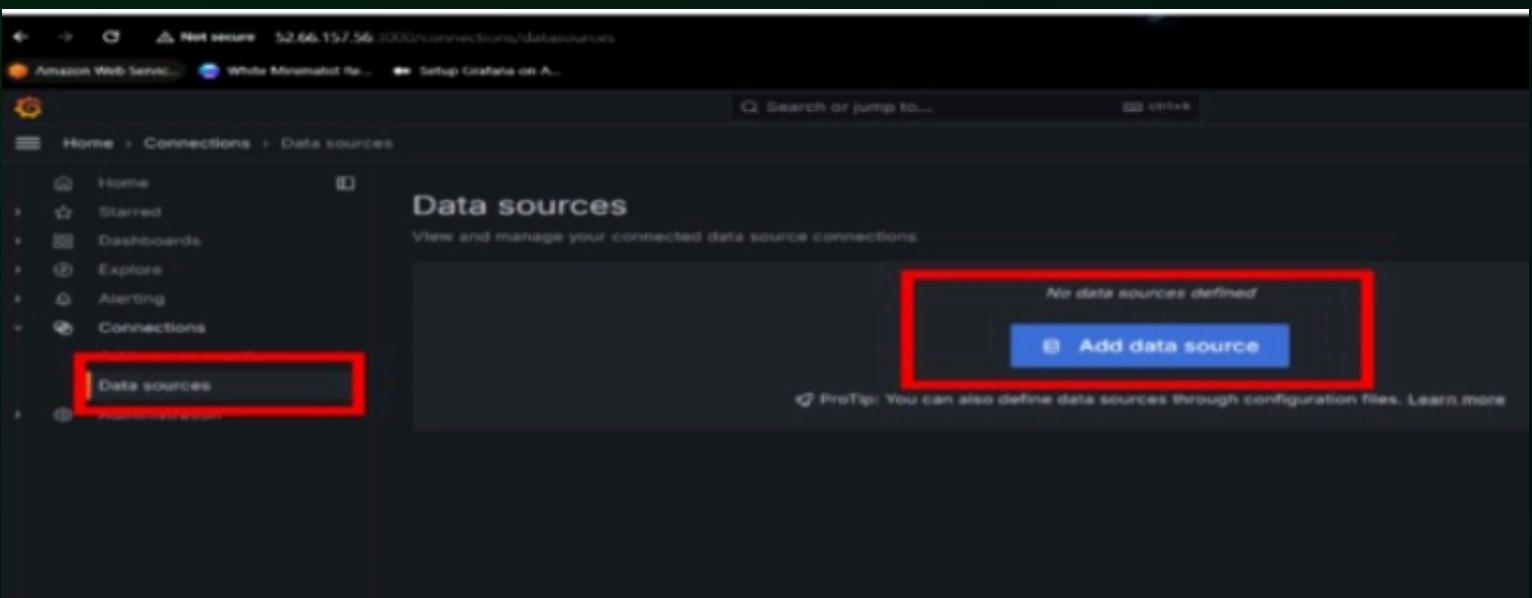
- For entrance in grafana we have to enter our instance private ip:3000 on any browser and search it



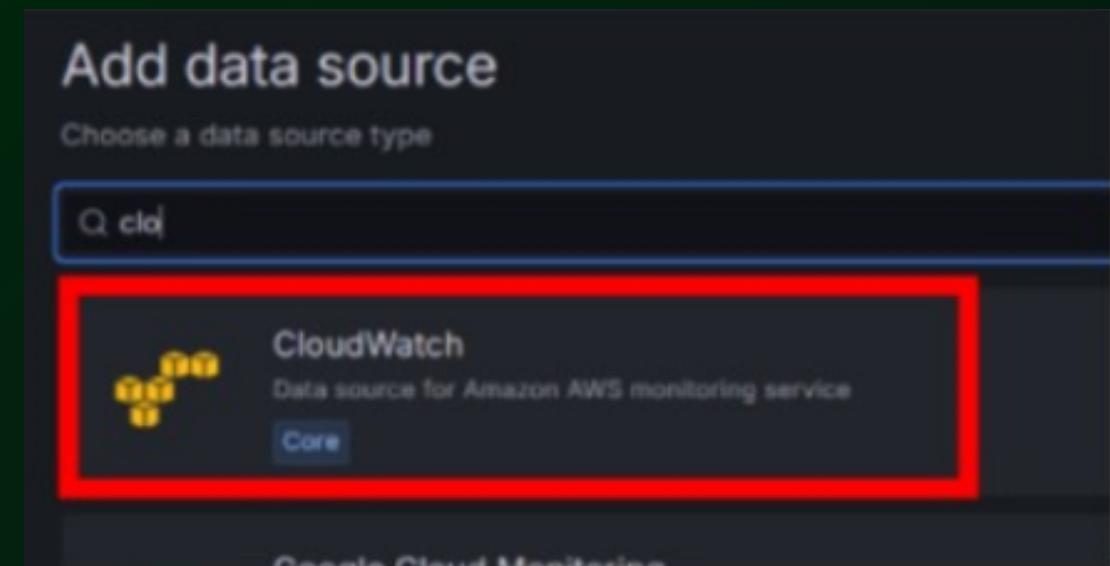
- Enter your username and password “admin”



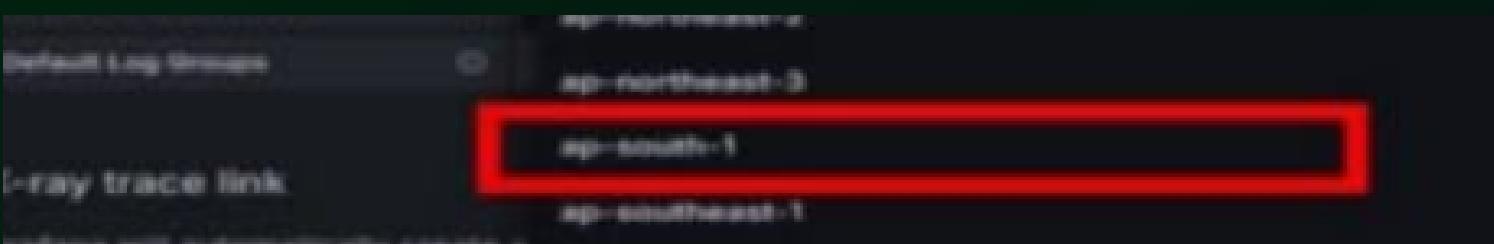
- Then go to data resources and click on “add data resources”



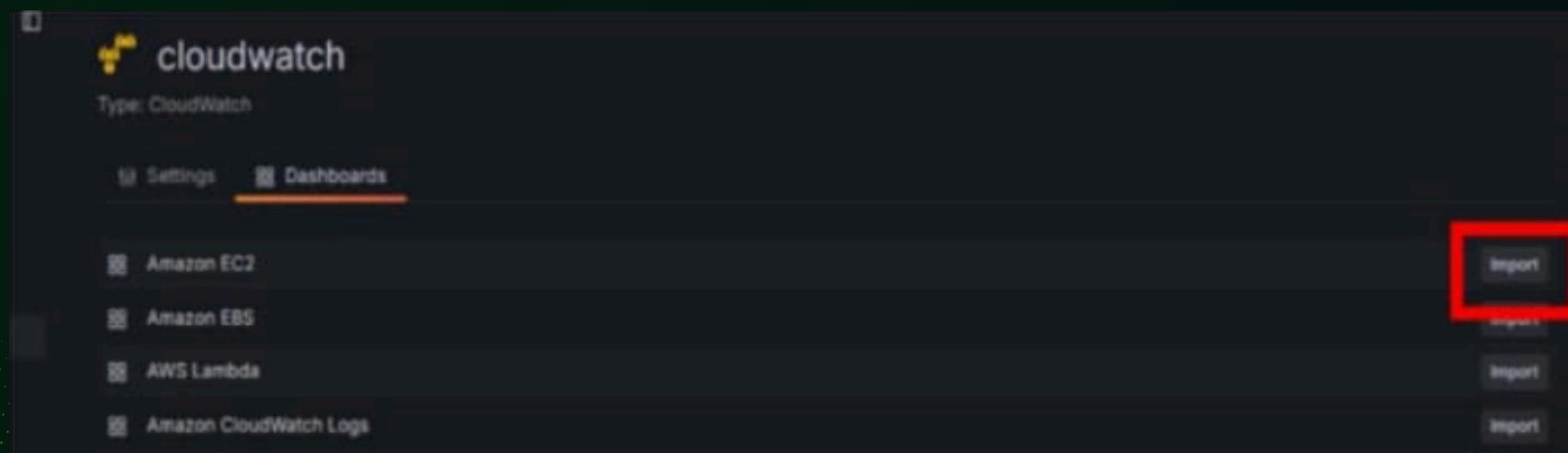
- Then search cloud watch



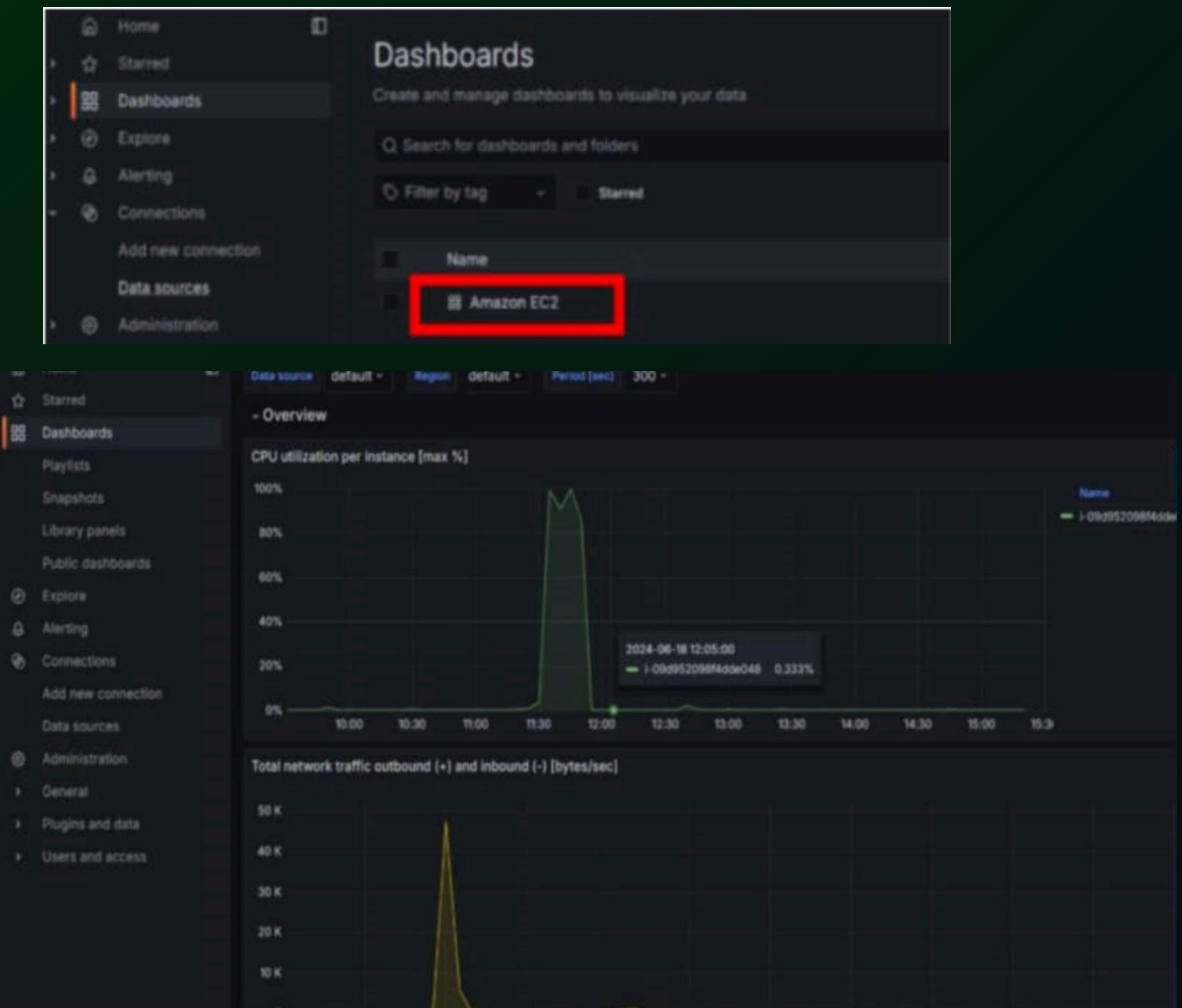
- Choose region ap-south-1



- Then go to dashboard and import amazon EC2



- Then go to dashboard and select amazon EC2







THANK YOU

CONTACT US

9336453059

www.amodaws.com

amodpathak51@gmail.com.com

E-396 KDA colony sujanpur kanpur,UP

SUBMITTED TO Mr. ABHINAV DWIVEDI

