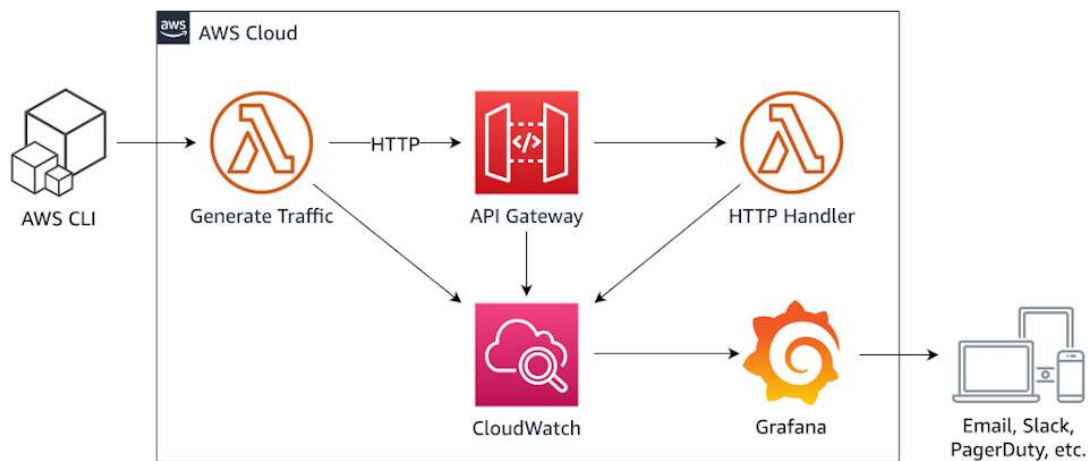


Integrate Grafana with Linux server for high CPU utilization and create a graph in Grafana.

Grafana

Grafana is opensource visualization and analytics software. It allows you to query, visualize, alert on, and explore your metrics, logs, and traces no matter where they are stored. It provides you with tools to turn your time-series database (TSDB) data into insightful graphs and visualizations.

Grafana ships with built-in support for Amazon CloudWatch. This topic describes queries, templates, variables, and other configuration specific to the CloudWatch data source.



Steps for Integrate Grafana with Linux server for high CPU utilization and create a graph in Grafana.

Step 1: Create an EC2 instance(ubuntu).

Step 2: installation of Grafana into instance

Step 3: creating policy.

Step 4: create a role.

Step 5: Modifying security rules.

Step 6: starting Grafana.

Step 7: Adding data source to Grafana.

Sign in to AWS Management Console

1.Click on the Open Console button, and you will get redirected to AWS Console in a new browser tab.

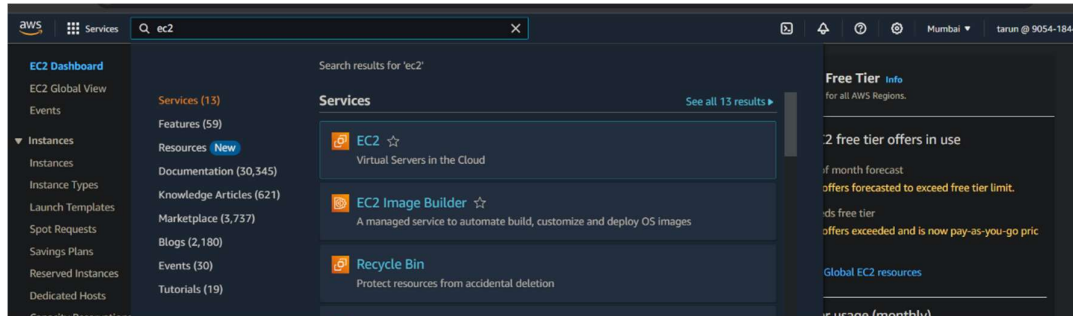
- **On the AWS sign-in page, Leave the Account ID as default. Never edit/remove the 12- digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.**
- **Now copy your User Name and Password in the Lab Console to the IAM Username and Password in AWS Console and click on the Sign in button**

2. Once Signed in to the AWS Management Console, Make the default AWS Region as US East (N. Virginia) us-east-1.

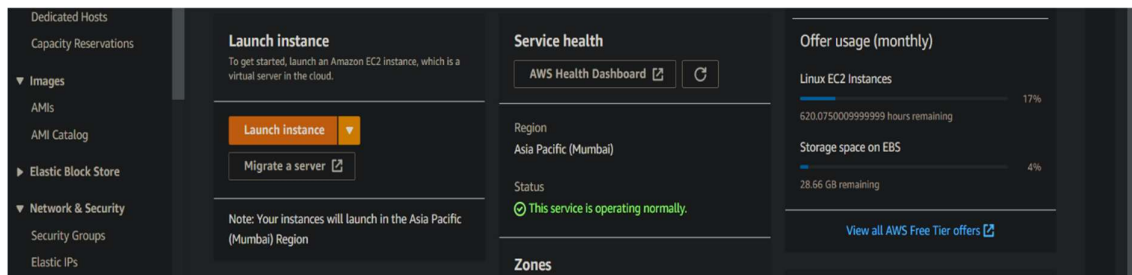
Step 1: Create an EC2 instance(ubuntu):

For creating an EC2 instance follow the following steps as shown in snapshots.

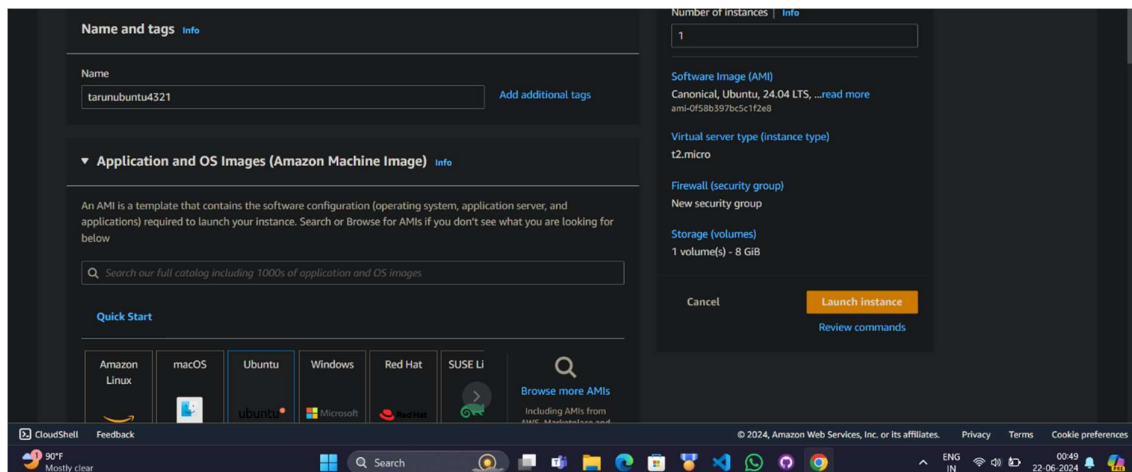
- On your AWS console search EC2 in services. And click on EC2.



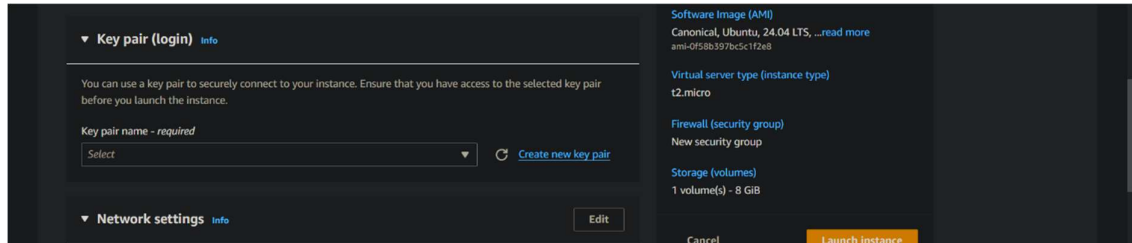
- Now click on launch instance so that you can make your instance



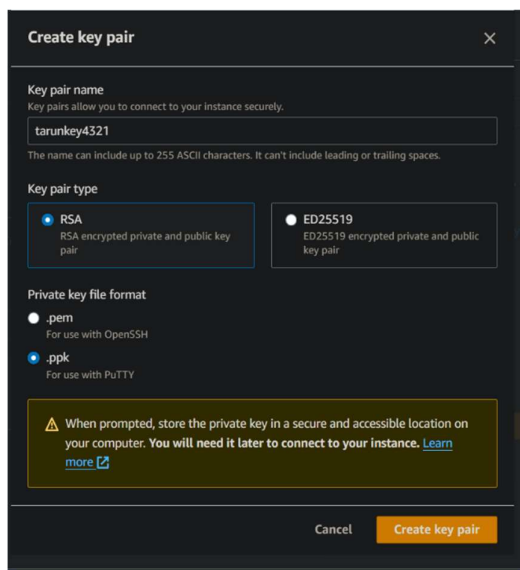
- Write the name of your instance and choose ubuntu as machine



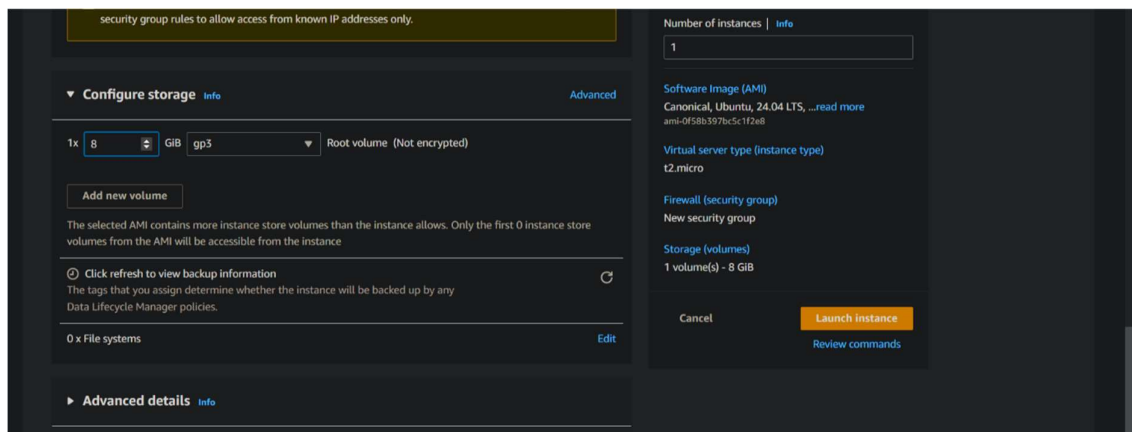
- Now click on create new key pair.



- Give your key pair a name and select RSA in key pair type and in key file format select .ppk and click on create key pair.



- Leave the other settings as default and launch an instance.



- Then open your instance and connect that instance by putty or on web browser.

- After connecting the instance follow the given command or read Grafana documentation for help.

Step 2: installation of Grafana into instance:

```
sudo apt-get install -y apt-transport-https software-properties-common wget
```

```
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-172-31-46-81:~$ sudo apt-get install -y apt-transport-https software-  
properties-common wget  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Note, selecting 'apt' instead of 'apt-transport-https'  
E: Unable to locate package software-properties-common
```

```
sudo mkdir -p /etc/apt/keyrings/  
wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee  
/etc/apt/keyrings/grafana.gpg >  
/dev/null
```

```
dev/null  
mkdir: invalid option -- 'q'  
Try 'mkdir --help' for more information.  
gpg: no valid OpenPGP data found.  
ubuntu@ip-172-31-46-81:~$ sudo mkdir -p /etc/apt/keyrings/  
ubuntu@ip-172-31-46-81:~$ wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings/grafana.gpg >/dev/null  
ubuntu@ip-172-31-46-81:~$
```

```
echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com  
stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
```

```
mkdir: invalid option -- 'q'  
Try 'mkdir --help' for more information.  
gpg: no valid OpenPGP data found.  
ubuntu@ip-172-31-46-81:~$ sudo mkdir -p /etc/apt/keyrings/  
ubuntu@ip-172-31-46-81:~$ wget -q -O - https://apt.grafana.com/gpg.key | gpg --dearmor | sudo tee /etc/apt/keyrings/grafana.gpg >/dev/null  
ubuntu@ip-172-31-46-81:~$ echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.l  
ist  
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main
```

- To update the list of the available packages

```
sudo apt-get update
```

```
ubuntu@ip-172-31-46-81:~$ sudo apt-get update  
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease [256 kB]  
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]  
Get:4 https://apt.grafana.com stable InRelease [7661 B]  
Get:5 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 Packages [1401 kB]  
Get:6 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]  
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main Translation-en [513 kB]  
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]  
Get:9 https://apt.grafana.com stable/main amd64 Packages [252 kB]  
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
```

- To install the latest enterprise release

```
sudo apt-get install grafana-enterprise
```

```
Preparing to unpack .../grafana-enterprise_11.0.0_amd64.deb ...
Unpacking grafana-enterprise (11.0.0) ...
Setting up musl:amd64 (1.2.4-2) ...
Setting up grafana-enterprise (11.0.0) ...
info: Selecting UID from range 100 to 999 ...

info: Adding system user `grafana' (UID 111) ...
info: Adding new user `grafana' (UID 111) with group `grafana' ...
info: Not creating home directory `/usr/share/grafana'.
### NOT starting on installation, please execute the following statements to configure grafana to start automatically using systemd
  sudo /bin/systemctl daemon-reload
  sudo /bin/systemctl enable grafana-server
### You can start grafana-server by executing
  sudo /bin/systemctl start grafana-server
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
```

- To start or enable server

```
sudo systemctl start grafana-Server.service
sudo systemctl enable grafana-Server.service
```

After that to check the status of the server write

```
sudo systemctl status grafana-server.service
```

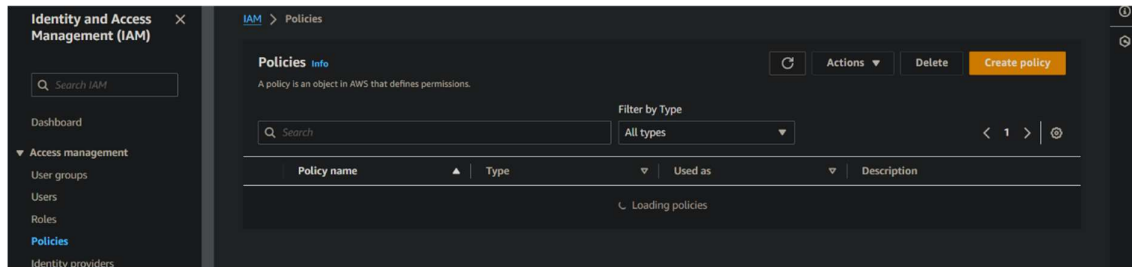
- now we can see that our server is running and active.

```
Executing: /usr/lib/systemd/systemd-sysv-install enable grafana-server
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service → /usr/lib/systemd/system/grafana-server.service.
ubuntu@ip-172-31-46-81:~$ sudo systemctl enable grafana-server.service
Synchronizing state of grafana-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable grafana-server
ubuntu@ip-172-31-46-81:~$ sudo systemctl status grafana-server
grafana-server.service - Grafana instance
   Loaded: loaded (/usr/lib/systemd/system/grafana-server.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-06-21 19:37:06 UTC; 6min ago
     Docs: http://docs.grafana.org
    Main PID: 2113 (grafana)
      Tasks: 10 (limit: 1130)
    Memory: 105.5M (peak: 113.6M)
       CPU: 2.958s
    CGroup: /system.slice/grafana-server.service
            └─2113 /usr/share/grafana/bin/grafana server --config=/etc/grafana/grafana.ini --pidfile=/run/grafana/grafana-server.pid --packaging=deb cfg:default>

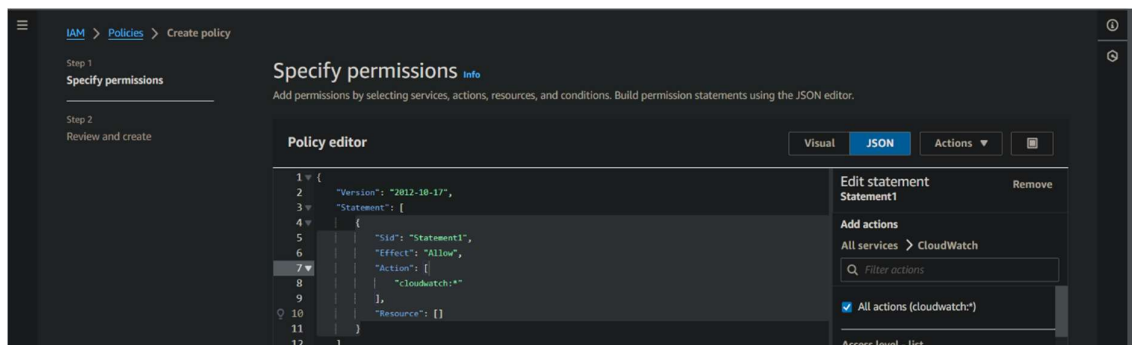
Jun 21 19:37:13 ip-172-31-46-81 grafana[2113]: logger=report t=2024-06-21T19:37:13.768100939Z level=warn msg="Scheduling and sending of reports disabled, SMTP is>
Jun 21 19:37:13 ip-172-31-46-81 grafana[2113]: logger=ngalert.multiorg.alertmanager t=2024-06-21T19:37:13.783342108Z level=info msg="Starting MultiOrg Alertmanag>
Jun 21 19:37:13 ip-172-31-46-81 grafana[2113]: logger=ngalert.scheduler t=2024-06-21T19:37:13.78339722Z level=info msg="Starting scheduler" tickInterval=10s max>
Jun 21 19:37:13 ip-172-31-46-81 grafana[2113]: logger=ticker t=2024-06-21T19:37:13.783873362Z level=info msg="starting first tick-2024-06-21T19:37:20Z
Jun 21 19:37:14 ip-172-31-46-81 grafana[2113]: logger=grafana.update.checker t=2024-06-21T19:37:14.208670441Z level=info msg="Update check succeeded" duration=47>
Jun 21 19:37:14 ip-172-31-46-81 grafana[2113]: logger=plugins.update.checker t=2024-06-21T19:37:14.22768318Z level=info msg="Update check succeeded" duration=489>
Jun 21 19:37:14 ip-172-31-46-81 grafana[2113]: logger=grafana-apiserver t=2024-06-21T19:37:14.231122981Z level=info msg="Adding GroupVersion playlist.grafana.app>
Jun 21 19:37:14 ip-172-31-46-81 grafana[2113]: logger=grafana-apiserver t=2024-06-21T19:37:14.23182367Z level=info msg="Adding GroupVersion featuretoggle.grafana>
Jun 21 19:37:14 ip-172-31-46-81 grafana[2113]: logger=plugin.angular detectorsprovider.dynamic t=2024-06-21T19:37:14.270204392Z level=info msg="Patterns update fi>
Jun 21 19:38:09 ip-172-31-46-81 grafana[2113]: logger=infra.usagstats t=2024-06-21T19:38:09.745752618Z level=info msg="Usage stats are ready to report"
lines 1-21/21 (END)
```

Step 3: creating policy:

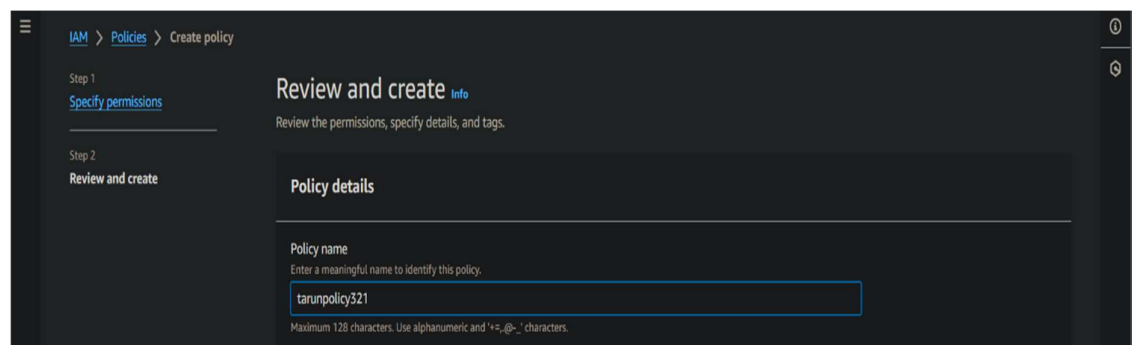
- Go to the IAM on your amazon dashboard where you can see the policies option in the left side click and then click on the create policy button on the right side in policies.



- Choose json in the specify permissions and in json clear the following statement that is already on the screen and select add new statement and then choose cloud watch with all action in the statement.

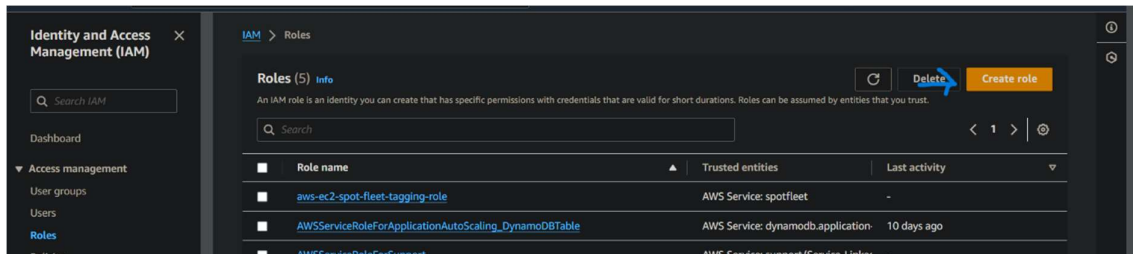


- In resources write “*” and the click on the next.
- In review and create section give your policy a unique name and click on the create policy button in the right bottom of the page.

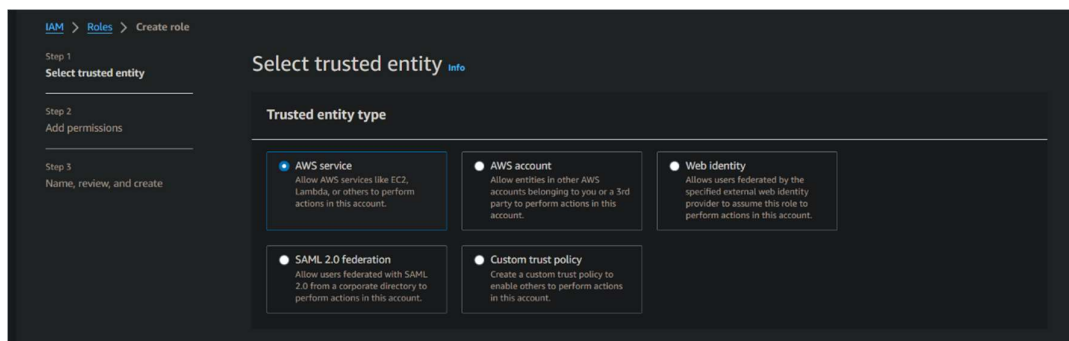


Step 4: create a role

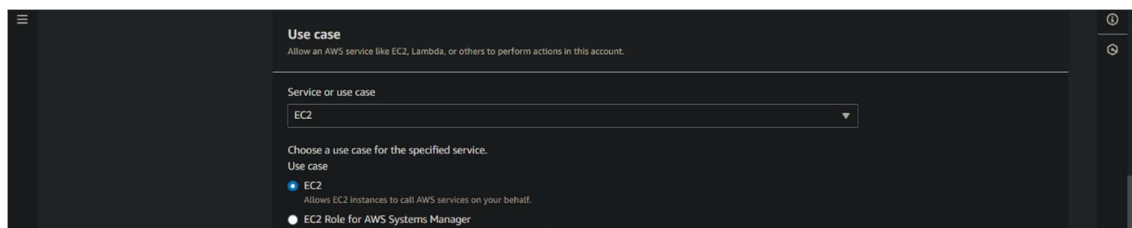
- Go to the roles in the IAM section of your amazon dashboard. And click on create policy.



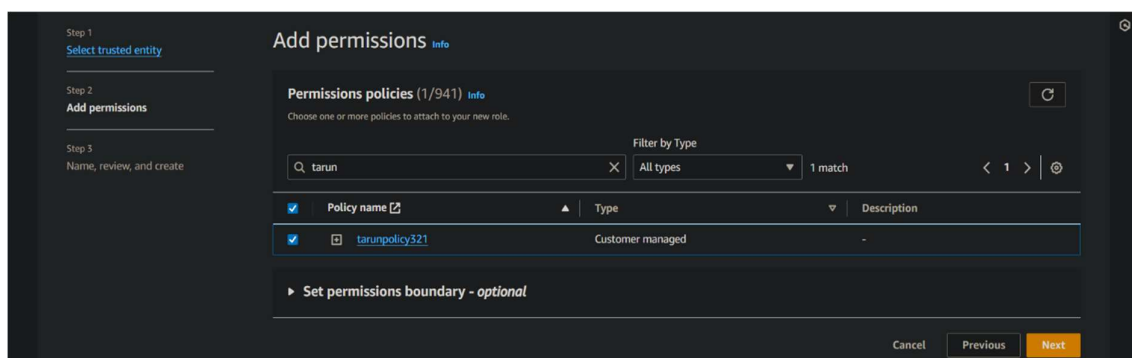
- In the select trusted entity select AWS service.



- In the use case select EC2 and click on the next button.



- In add permission select your policy the you already created.



- In name, review and create section give your role a name and click on create role button.

Step 1

[Select trusted entity](#)

Step 2

[Add permissions](#)

Step 3

Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+', '@', '-', '_' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+., @-/[()!\$%&'":~<>`

Step 5: Modifying security rules

- After creating your role and policy go to your instance.
- Click on your instance and scroll down to the security. In the security click on the security group in the blue coloured link.

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

am:aws:ec2:ap-south-1:905418447105:instance/i-063690d3b1fe331f6

Details

Status and alarms

Monitoring

Security

Networking

Storage

Tags

▼ Security details

IAM Role

—

Owner ID

📄 905418447105

Launch time

Sat Jun 22 2024 00:52:10 GMT+0530 (India Standard Time)

Security groups

🔗 sg-048259527e438ab0e (launch-wizard-14)

▼ Inbound rules

- In the security group scroll down to the inbound rule and then click on the edit inbound rules.

EC2 Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

EC2 > Security Groups > sg-048259527e438ab0e - launch-wizard-14

sg-048259527e438ab0e - launch-wizard-14

Actions

Details

<div>Security group name</div> <div>launch-wizard-14</div>	<div>Security group ID</div> <div>sg-048259527e438ab0e</div>	<div>Description</div> <div>launch-wizard-14 created 2024-06-21T19:18:25.018Z</div>	<div>VPC ID</div> <div>vpc-0fd125980362775a9</div>
<div>Owner</div> <div>905418447105</div>	<div>Inbound rules count</div> <div>1 Permission entry</div>	<div>Outbound rules count</div> <div>1 Permission entry</div>	

Inbound rules

Outbound rules

Tags

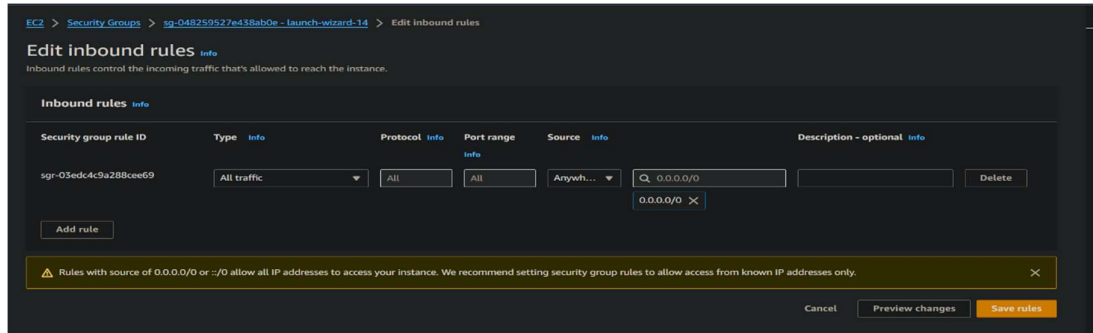
Inbound rules (1)

Refresh

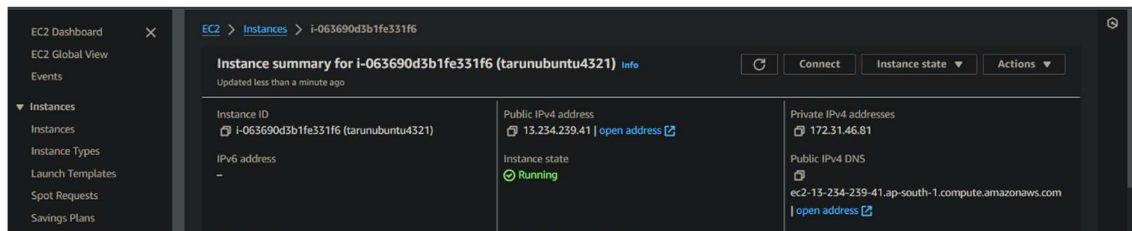
Manage tags

Edit inbound rules

- In edit inbound rules create rule with all traffic in type and select 0.0.0.0/0 in the source section and then click on the save rule.

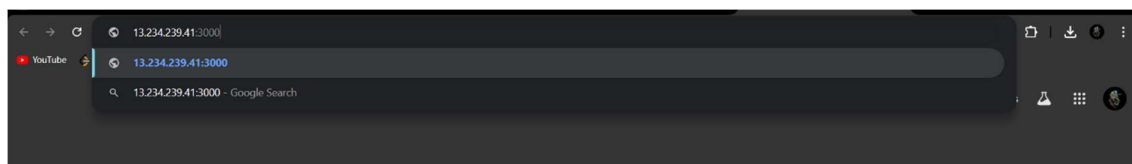


Now copy the public IPv4 address of your instance.

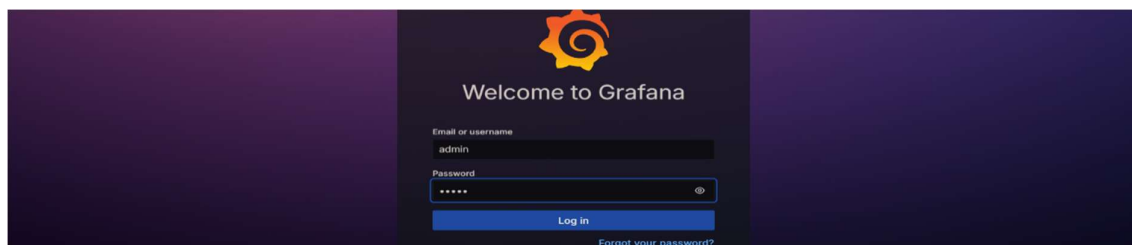


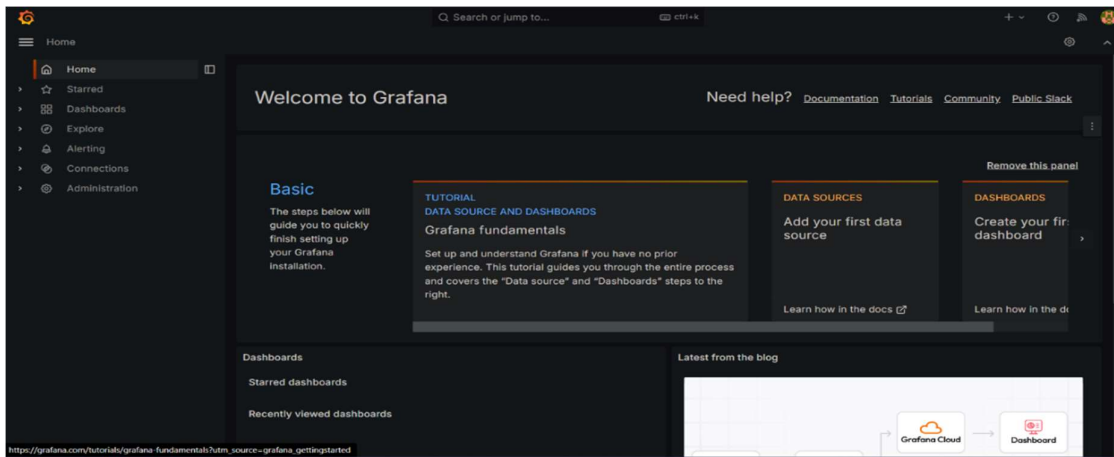
Step 6: starting Grafana

- Paste the copied IP of your instance in browser and write :3000 after the IP address.



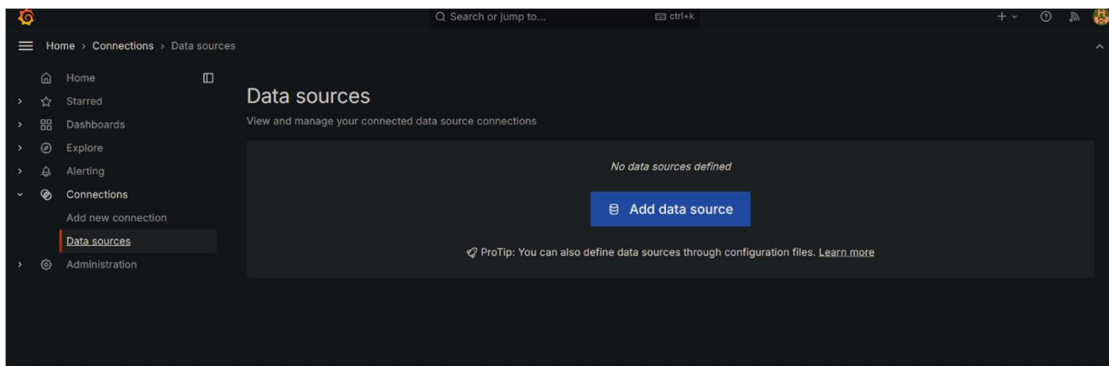
- Then login in Grafana by the help of the below screen short.



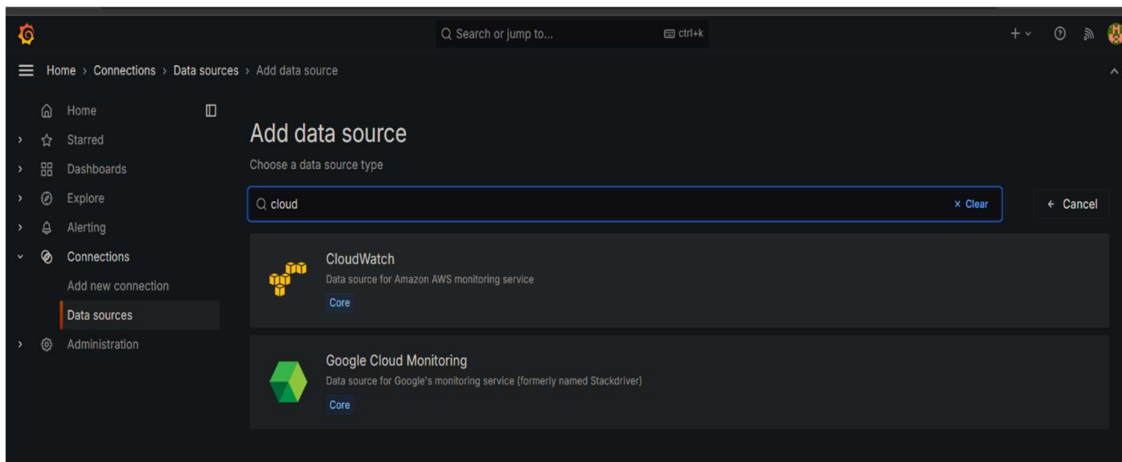


Step 7: Adding data source to Grafana

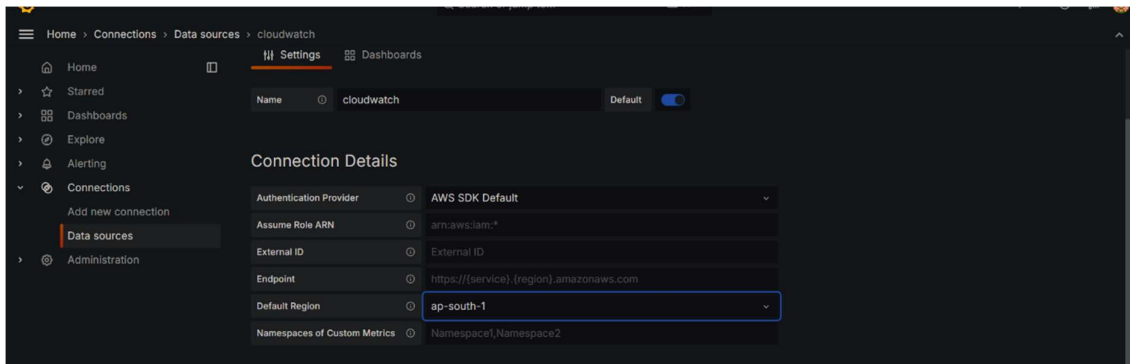
- Go to the connections in connection select data sources and then click on add data source.



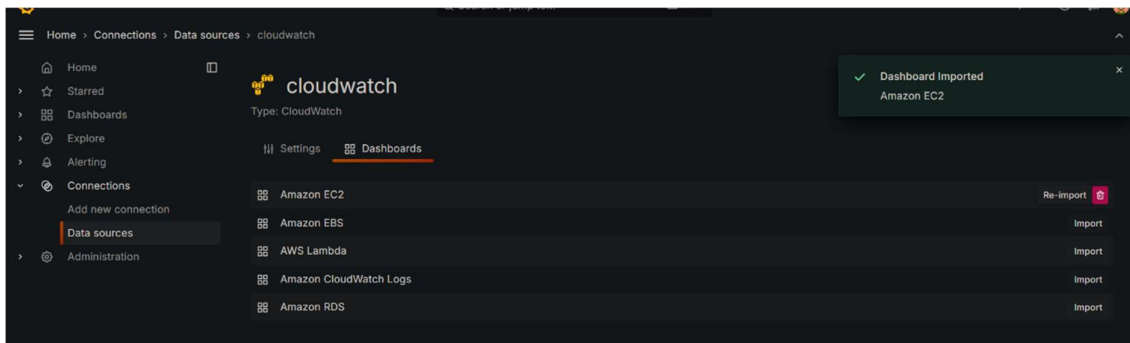
- Search cloud watch on the choose a data source type.



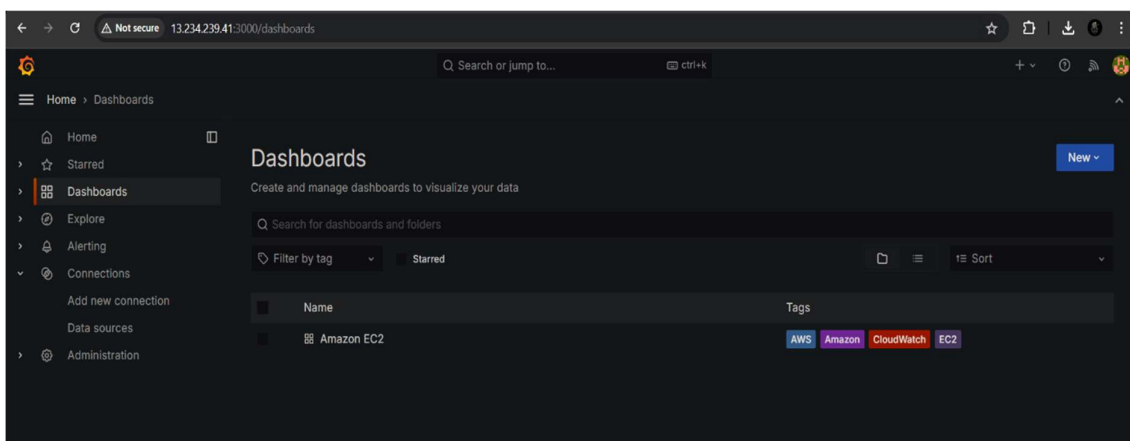
- In cloud watch go the settings in settings select your region in the connection details.



- In the cloud watch dashboard import Amazon EC2.

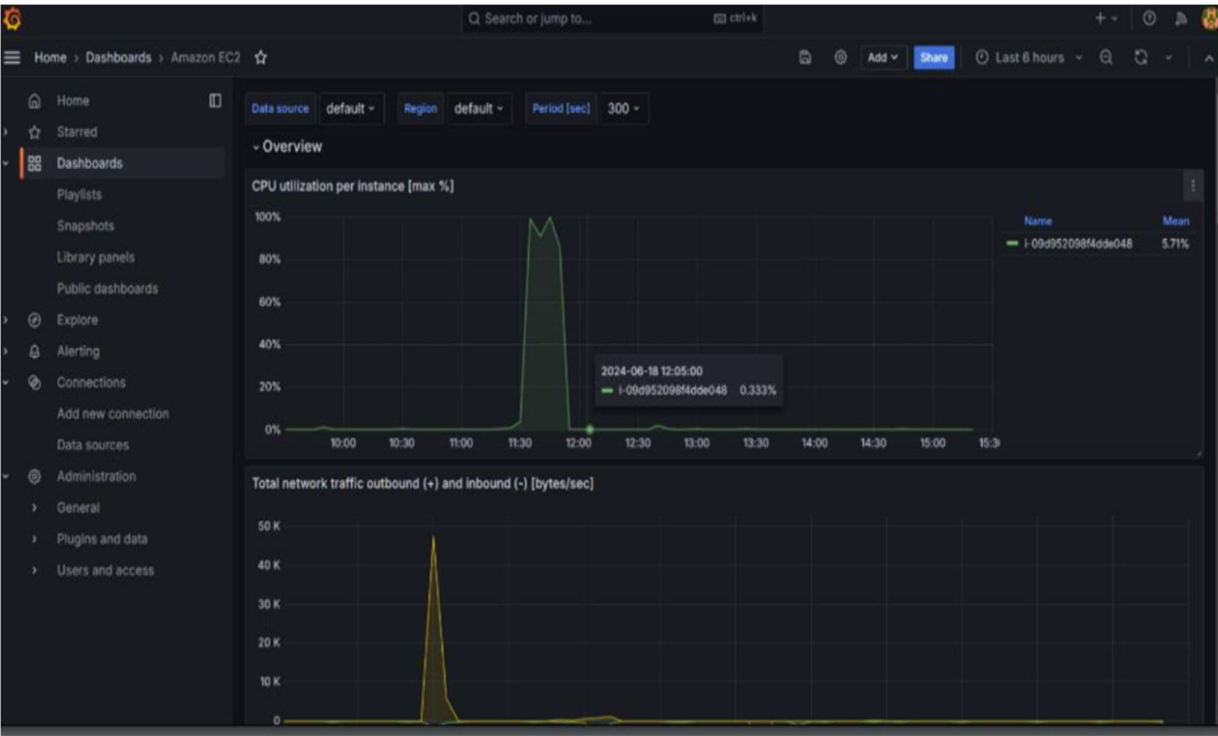


- After that go to the dashboard and click on the Amazon EC2



CPU utilization graph

❖ Graph of the CPU utilization in Grafana.



❖ Graph of the network traffic in Grafana.



❖ Detailed graph of the network traffic in Grafana

