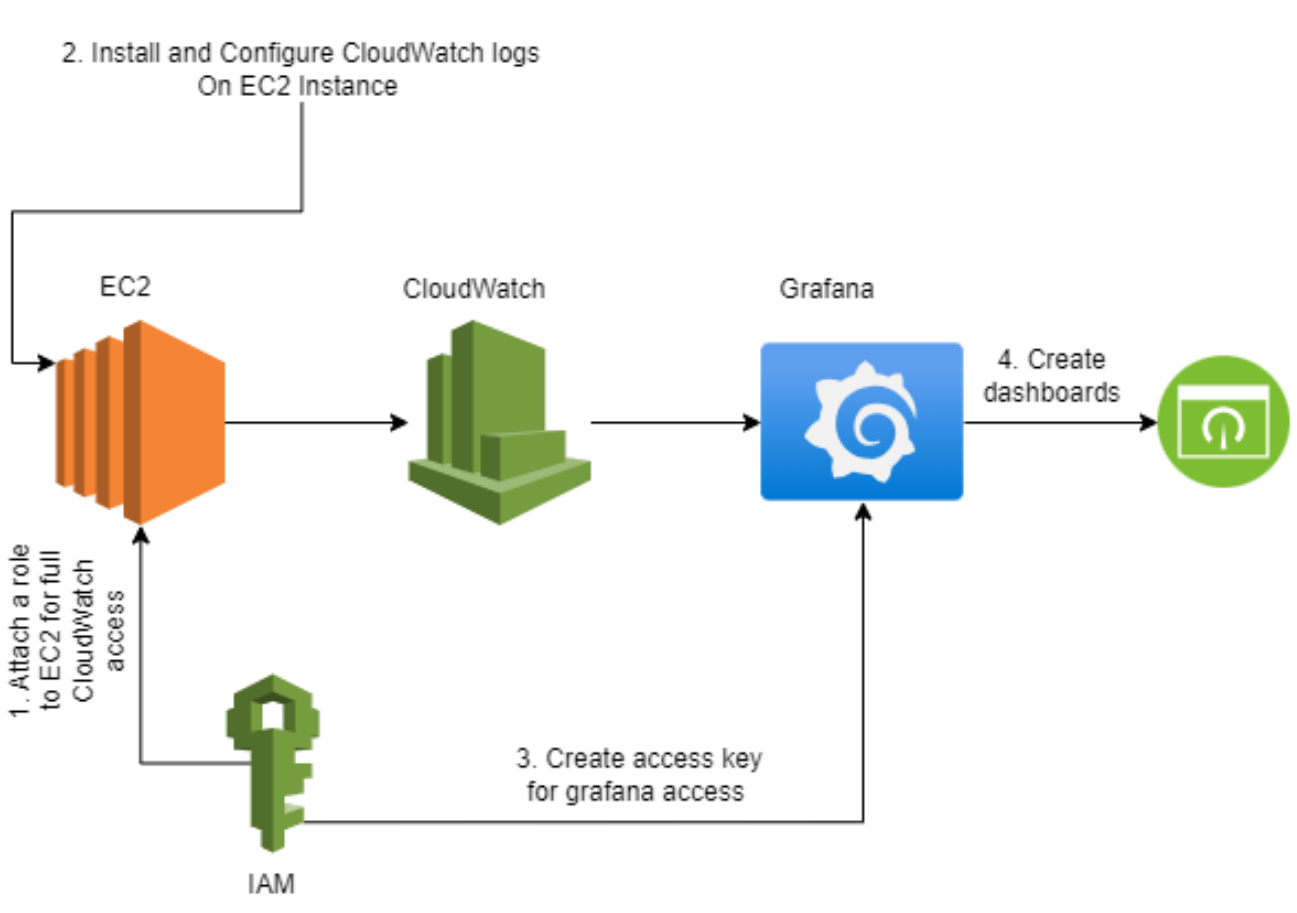
Montioring EC2 Instance Logs Using CloudWatch And Grafana

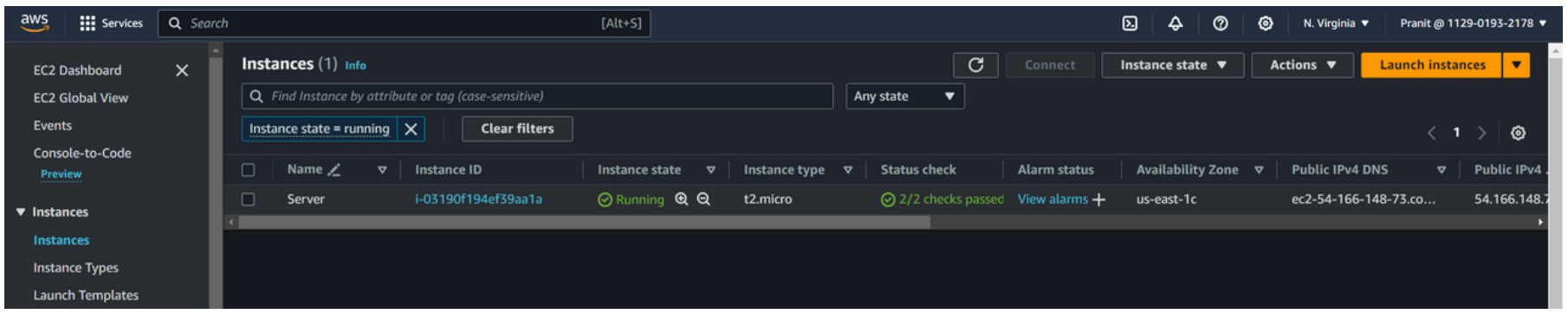
Procedure Breakdown

- Here first an EC2 instance is created . Then attached a IAM role having CloudWatchFullAccess policy . Then installed and enabled CloudWatch logs on the EC2 instance .
- Then created access keys for grafana .
- Then started a grafana server using docker at port 3000 and logged in using admin as both username and password .
- Then created a data source using CloudWatch . Here the access and security key along with default region is mentioned .
- After this some scripts run on the EC2 instance to create logs .
- Finally created some dashboards and observed the EC2 instance logs using grafana .



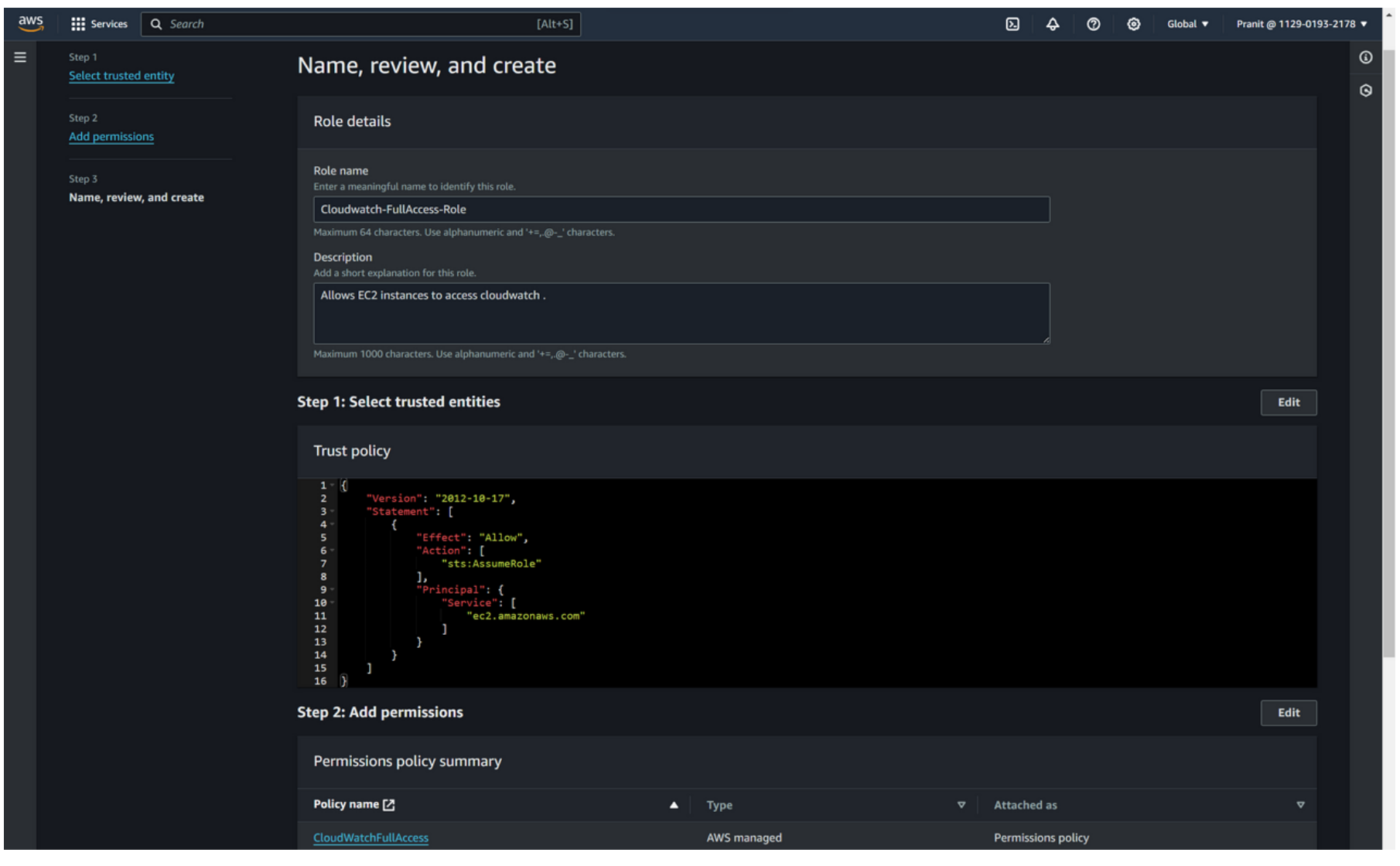
1.Created an EC2 Instance.

- Here i have used Amazon Linux 2 AMI .
- I have used t2.micro and rest things are in default .



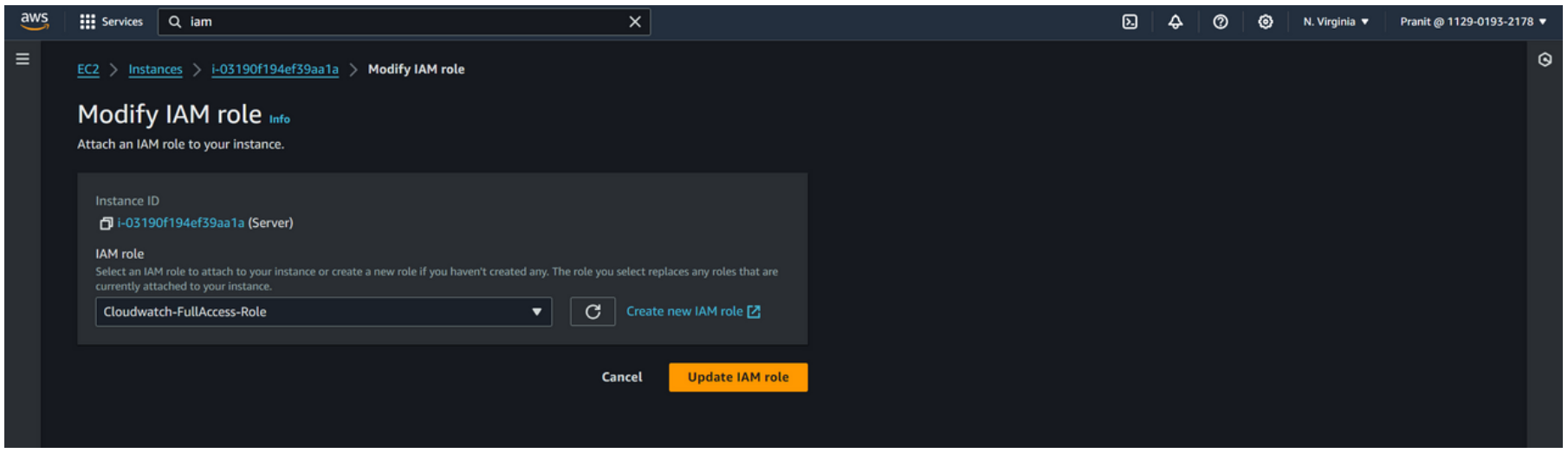
2.Created an IAM role having CloudWatch Full Access policy

- First i moved to the IAM dashboard and selected create new role .
- Then attached CloudWatchFullAccess policy to the role .



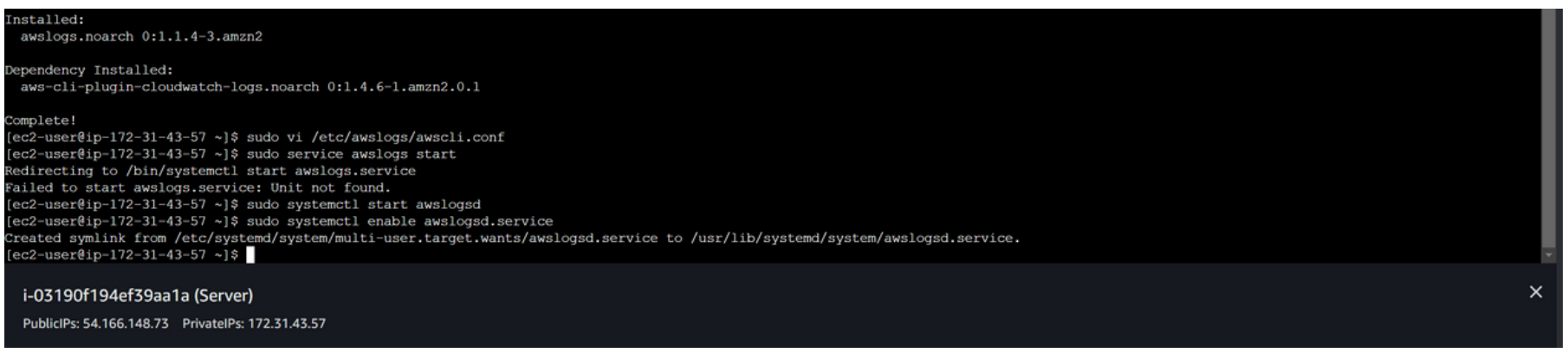
3.Attached the new IAM role created to the EC2 instance .

- Here first i moved to EC2 dashboard and then selected actions.(top right corner)
- Then selected security .
- Then selected Modify IAM Role .After this i finally attached the new role to the EC2 instance .



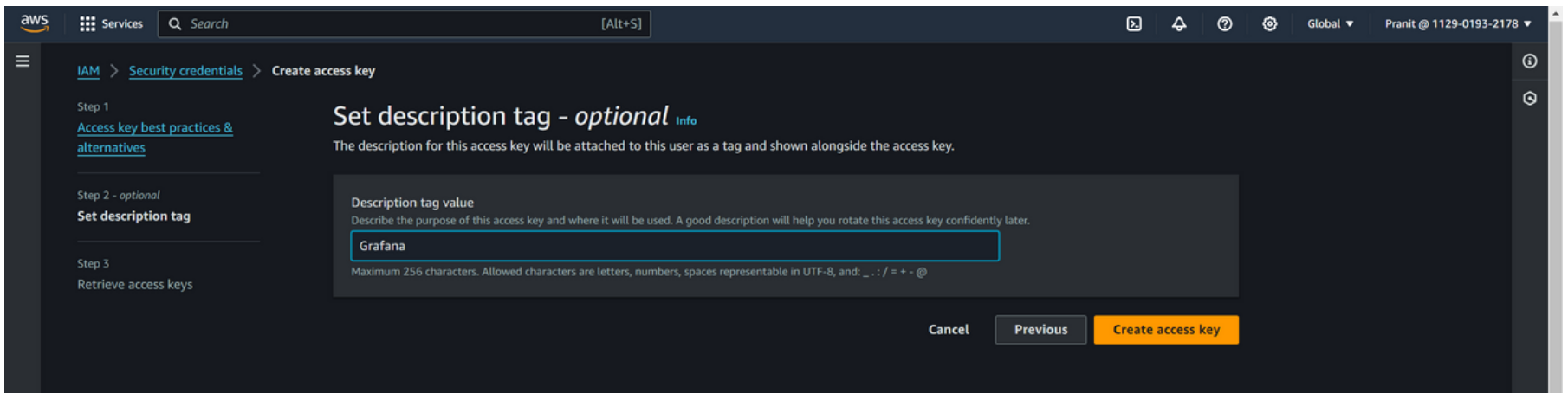
4.Installed CloudWatch logs on EC2 instance .

- Here first i connected the EC2 instance .
- Then used the following commands to install CloudWatch logs on EC2 instance .
- **sudo yum update -y**
- **sudo yum install -y awslogs**
- Here in the configuration file changed to the required region . (use **sudo vi /etc/awslogs/awscli.conf**)
- **sudo systemctl start awslogsd**
- **sudo systemctl enable awslogsd.service**



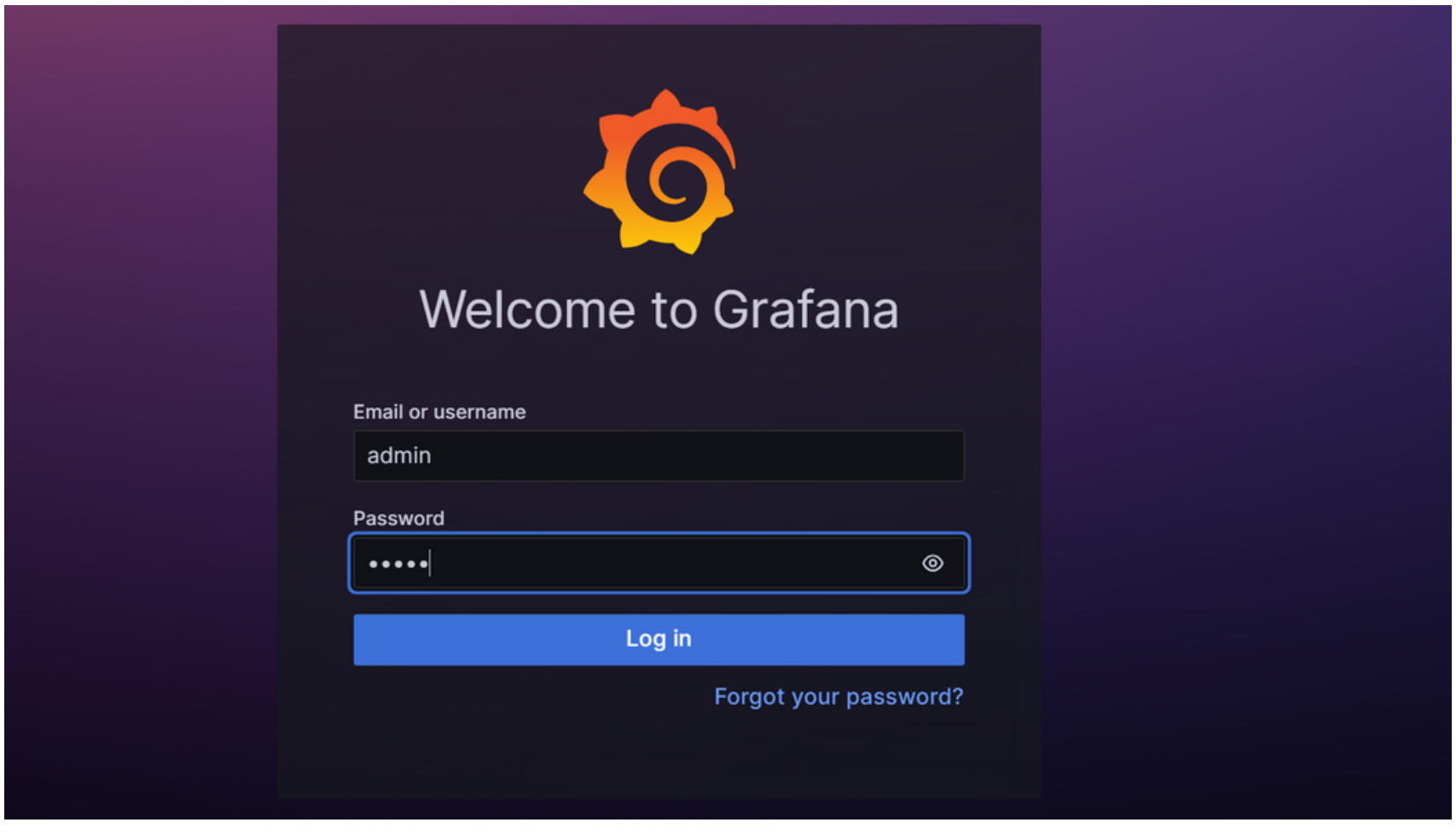
5.Created access keys for grafana.

- Here first i moved to IAM dashboard and then selected My Security Credential (at middle right part of the page).
- I have used t2.micro and rest things are in default .



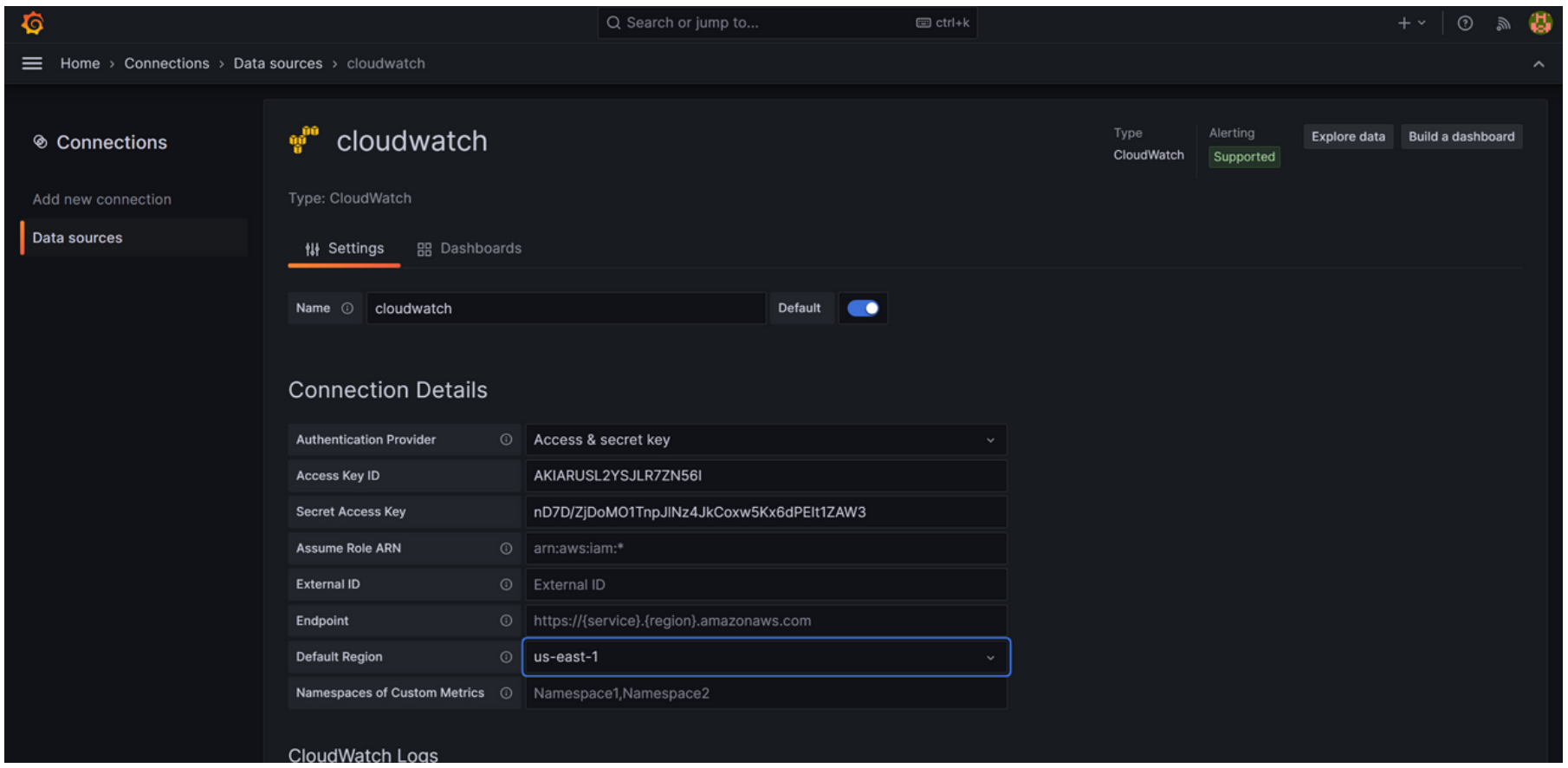
6.Started grafana using docker and accessed through port 3000 .

- Here i first make sure that docker is running .
- Then using the command **docker run -d --name grafana -p 3000:3000 grafana/grafana** started the grafana .
- Then accessed the grafana using port 3000 .
- Here used the **default username admin** and **default password admin** to login into the grafana .



7.Created a data source using CloudWatch.

- Here i have given the access and security keys
- Then mentioned the region i am using .
- Then save and test .



8.Created some scripts that will run 'Hello!!!!' continuously and store it in the logs file .

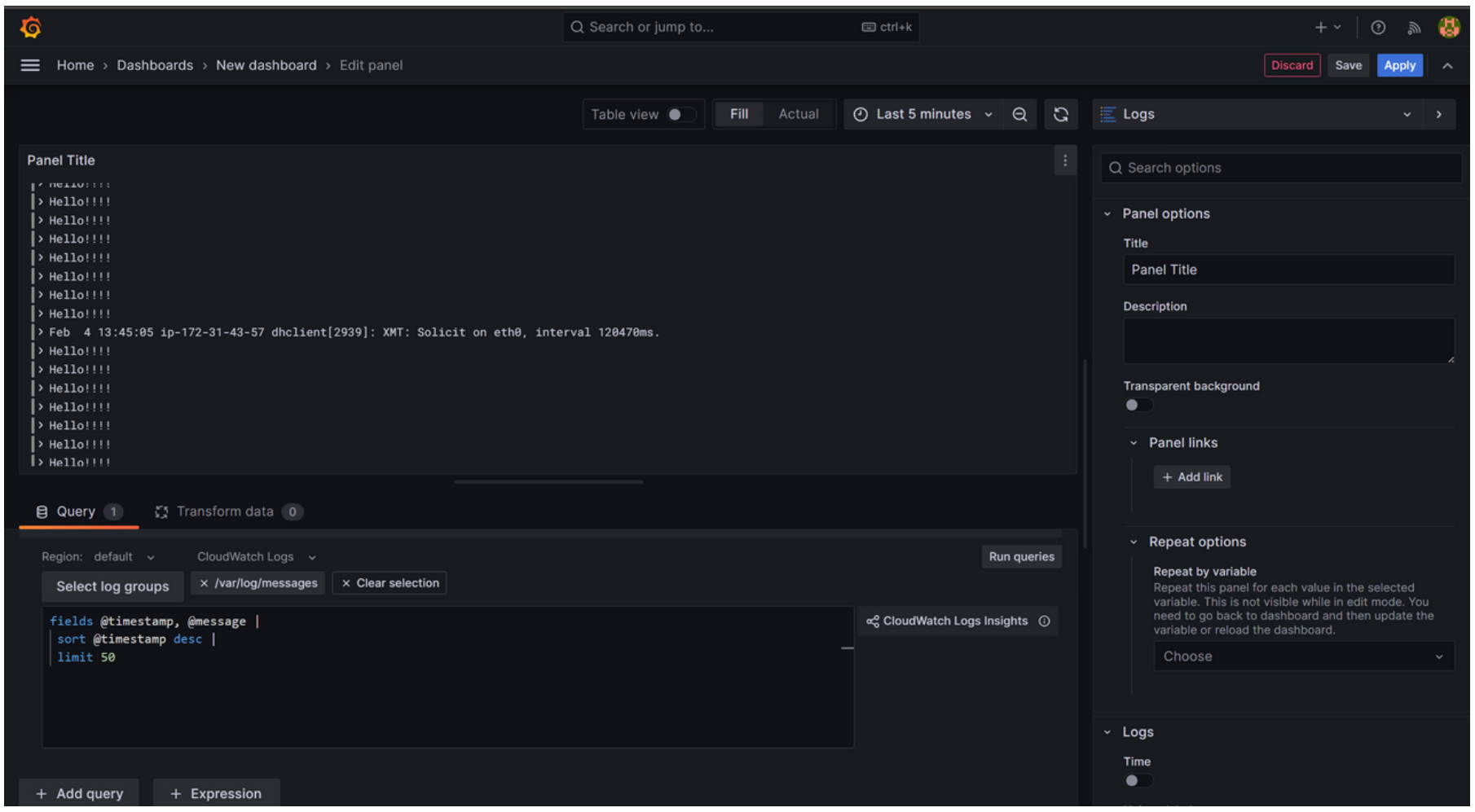
- Here i created a bash script .

```
#!/bin/bash

LOG_FILE="/var/log/messages"

while true; do
   echo "Hello!!!!"
   echo "Hello!!!!" >> "$LOG_FILE"
   sleep 1
done
```

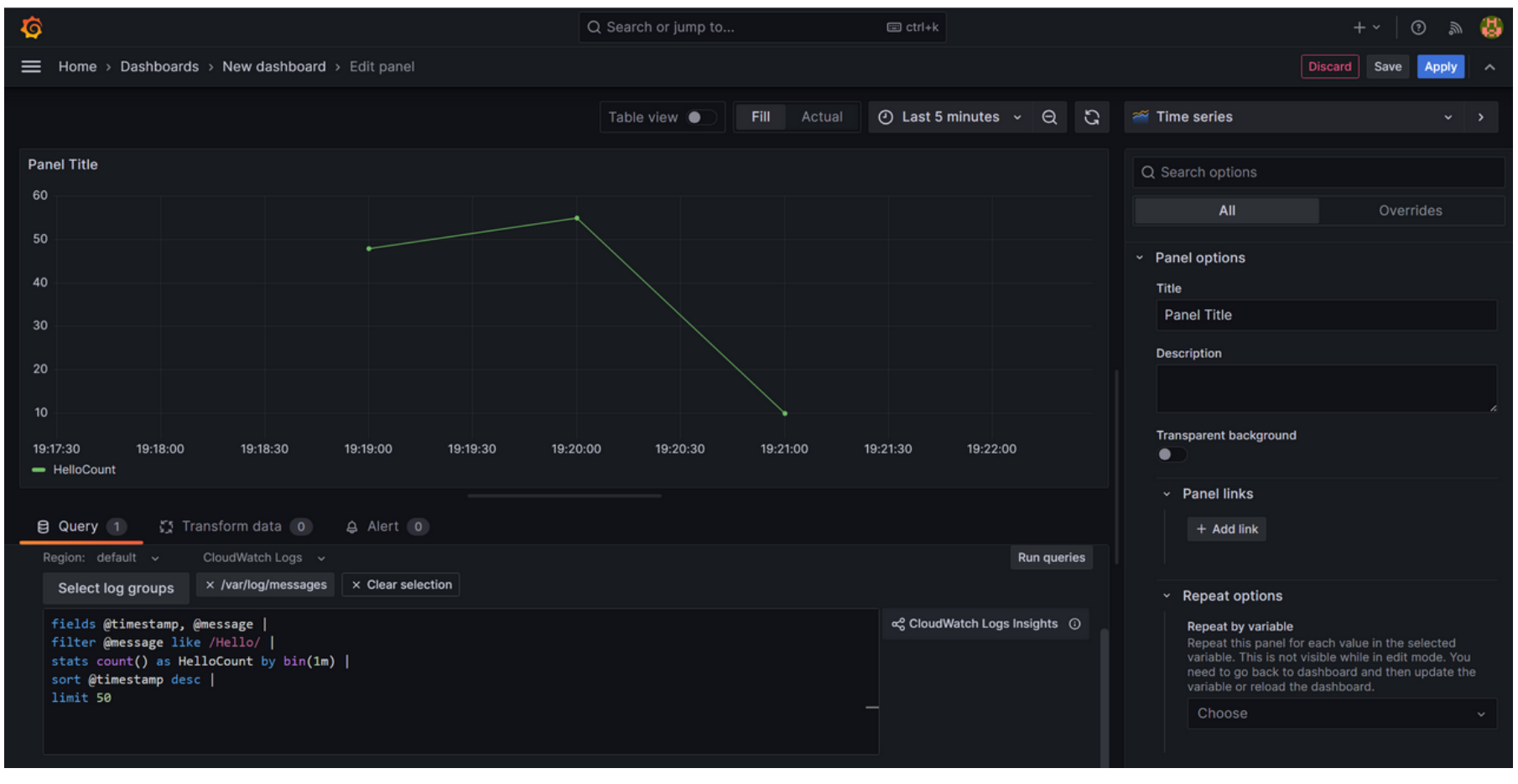
- Then given executable permission to the bash script using the command **chmod +x demo.sh**
- Then executed the bash script using the command **sudo nohup ./demo.sh > /dev/null 2>&1 &**

9.Created dashboard in grafana to see the logs of EC2 instance .

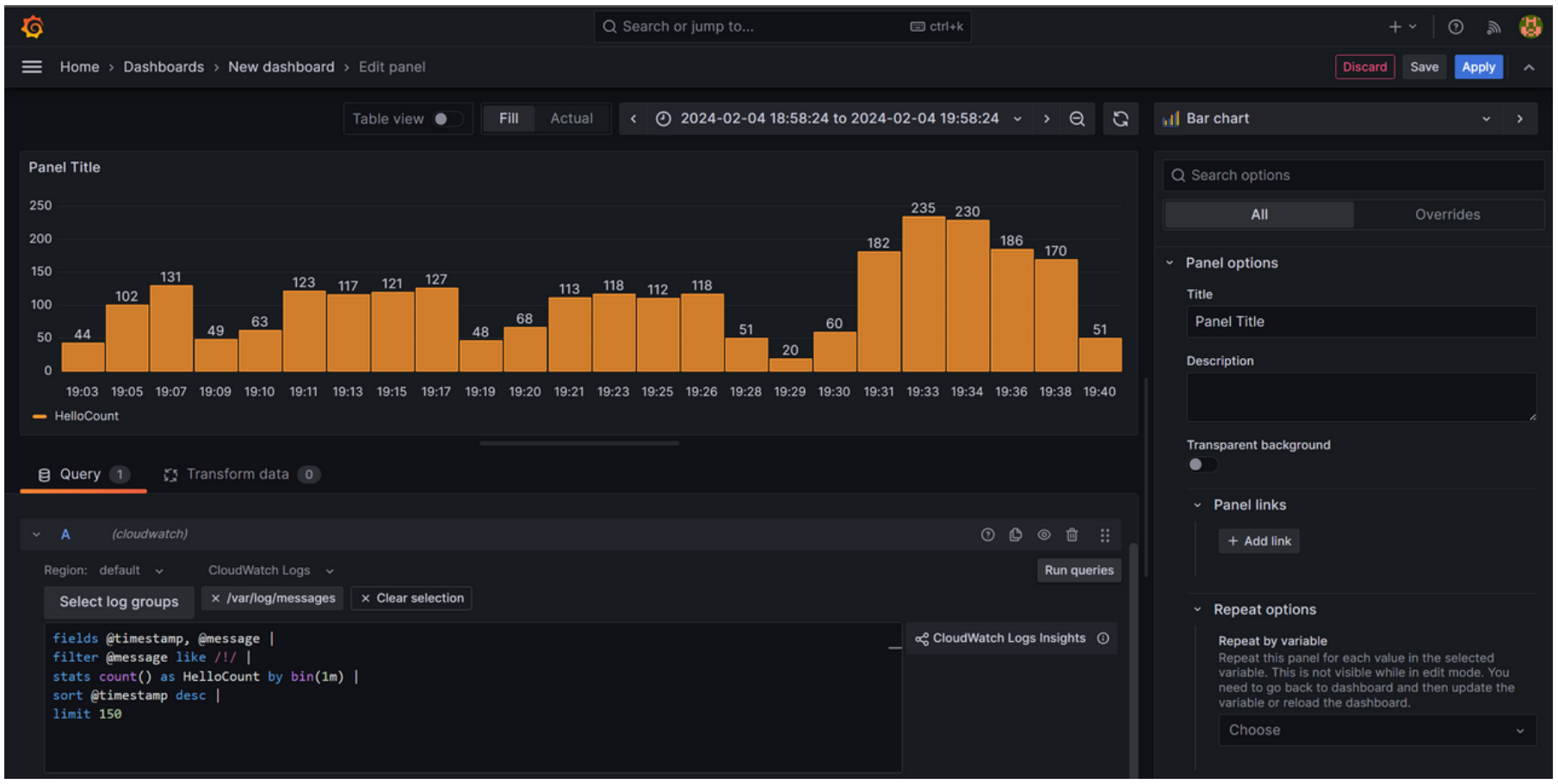
- The below dashboard shows the logs.



- The below dashboard counts the number of time Hello appeared in the logs .



- The below dashboard counts the number of times “!” comes in the message . .



- The below dashboard counts the number of times “Hello” comes in the message . .