

Project -3

Integrate Grafana with Linux Server for high cpu utilization and create a graph in Grafana

Table of content :-

- Introduction
- What's Grafana?
- Grafana's step-by-step installation

INTRODUCTION

In modern IT infrastructure, real-time monitoring and visualization of system performance is crucial. This project focuses on integrating **Grafana**, an open-source analytics and visualization tool, with a **Linux server running on AWS EC2**. The aim is to monitor **CPU utilization** using **Prometheus** and **Node Exporter**, collect metrics, and visualize them on a dynamic Grafana dashboard.

By doing so, system administrators and developers can track resource usage, detect bottlenecks, and ensure system reliability. This setup also introduces students to industry-level monitoring practices using open-source technologies on cloud infrastructure.

WHAT IS GRAFANA

Grafana is an open-source data visualization and monitoring tool used to analyze and display metrics from various data sources like Prometheus, InfluxDB, Graphite, MySQL, and more. It allows users to create interactive dashboards with real-time graphs, charts, and alerts to monitor the health and performance of systems, applications, and infrastructure.

Grafana is widely used in DevOps and IT operations for:

- Monitoring server resources (CPU, memory, disk usage)
- Observing cloud services and Kubernetes clusters
- Alerting on performance issues
- Creating custom dashboards for business analytics

With its user-friendly interface and plugin support, Grafana is a powerful tool for converting complex data into insightful visualizations.

▪ Step-by-Step Setup

1. launch instance.

- Choose Ubuntu 22.04 LTS.
- Select an instance type (t2.micro for testing).
- Create or use a key pair (use .ppk if using PuTTY).
- Open ports in Security Group:
 - SSH (22)
 - HTTP (80)
 - Custom TCP 3000 (Grafana)
 - Custom TCP 9090 (Prometheus)
 - Custom TCP 9100 (Node Exporter)

2. Connect to EC2 Using PuTTY

Use the public IP of the EC2 instance and connect using PuTTY with the .ppk private key.

Launch an instance [Info](#)

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

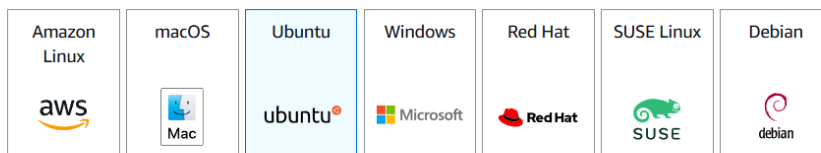
[Add additional tags](#)

▼ 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

Recents

Quick Start



[Browse more AMIs](#)
Including AMIs from
AWS, Marketplace and
the Community

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

mywebabcd

The name can include up to 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

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠ 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](#)

Cancel

Create key pair

<div>Source type Info</div> <div>Custom</div>	<div>Source Info</div> <div><div>Q Add CIDR, prefix list or security group</div><div>0.0.0.0/0</div></div>	<div>Description - optional Info</div> <div>e.g. SSH for admin desktop</div>
<div>▼ Security group rule 3 (TCP, 9090, 0.0.0.0/0)</div>		
<div>Type Info</div> <div>Custom TCP</div>	<div>Protocol Info</div> <div>TCP</div>	<div>Port range Info</div> <div>9090</div>
<div>Source type Info</div> <div>Custom</div>	<div>Source Info</div> <div><div>Q Add CIDR, prefix list or security group</div><div>0.0.0.0/0</div></div>	<div>Description - optional Info</div> <div>e.g. SSH for admin desktop</div>
<div>▼ Security group rule 4 (TCP, 9100, 0.0.0.0/0)</div>		
<div>Type Info</div> <div>Custom TCP</div>	<div>Protocol Info</div> <div>TCP</div>	<div>Port range Info</div> <div>9100</div>
<div>Source type Info</div> <div>Custom</div>	<div>Source Info</div> <div><div>Q Add CIDR, prefix list or security group</div><div>0.0.0.0/0</div></div>	<div>Description - optional Info</div> <div>e.g. SSH for admin desktop</div>

Now Launch instance

After launching the instances copy the public ip address of your instance and connect it with putty and login as :ubuntu and then press enter

```
login as: ubuntu
* Authenticating with public key "grafanakeypair"
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/pro

System information as of Wed Jun 25 14:25:40 UTC 2025

System load:  0.03          Processes:            106
Usage of /:   25.4% of 6.71GB Users logged in:          0
Memory usage: 21%          IPv4 address for enx0: 172.31.13.140
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
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-172-31-13-140:~$
```

- After this step run all these commands :-

[SUDO APT UPDATE &&SUDO APT UPGRADE -Y](#)

[2. WGET -Q -O - HTTPS://PACKAGES.GRAFANA.COM/GPG.KEY | SUDO APT-KEY ADD -](#)

[3. ECHO "DEB HTTPS://PACKAGES.GRAFANA.COM/OSS/DEB STABLE MAIN" | SUDO TEE /ETC/APT/SOURCES.LIST.D/GRAFANA.LIST](#)

[4. SUDO APT-GET INSTALL -Y APT-TRANSPORT-HTTPS](#)

[SUDO APT-GET INSTALL -Y SOFTWARE-PROPERTIES-COMMON WGET](#)

[WGET -Q -O - HTTPS://PACKAGES.GRAFANA.COM/GPG.KEY | SUDO APT-KEY ADD -](#)

[ECHO "DEB HTTPS://PACKAGES.GRAFANA.COM/OSS/DEB STABLE MAIN" | SUDO TEE /ETC/APT/SOURCES.LIST.D/GRAFANA.LIST](#)

[SUDO APT-GET UPDATE](#)

[SUDO APT-GET INSTALL GRAFANA](#)

[5. SUDOSYSTEMCTL DAEMON-REEXEC](#)

[SUDOSYSTEMCTL START GRAFANA-SERVER](#)

[SUDOSYSTEMCTL ENABLE GRAFANA-SERVER](#)

[6. LS /LIB/SYSTEMD/SYSTEM/GRAFANA-SERVER.SERVICE](#)

[7. SUDO APT REMOVE GRAFANA](#)

[SUDO APT UPDATE](#)

[SUDO APT INSTALL GRAFANA](#)

[8. SUDO APT UPDATE &&SUDO APT UPGRADE –](#)

[9. WGET -Q -O - HTTPS://PACKAGES.GRAFANA.COM/GPG.KEY | SUDO APT-KEY ADD -](#)

[10. ECHO "DEB HTTPS://PACKAGES.GRAFANA.COM/OSS/DEB STABLE MAIN" | SUDO TEE /ETC/APT/SOURCES.LIST.D/GRAFANA.LIST](#)

[11. SUDO APT UPDATE](#)

[12. SUDO APT INSTALL GRAFANA -Y](#)

[13. SUDOSYSTEMCTL START GRAFANA-SERVER](#)

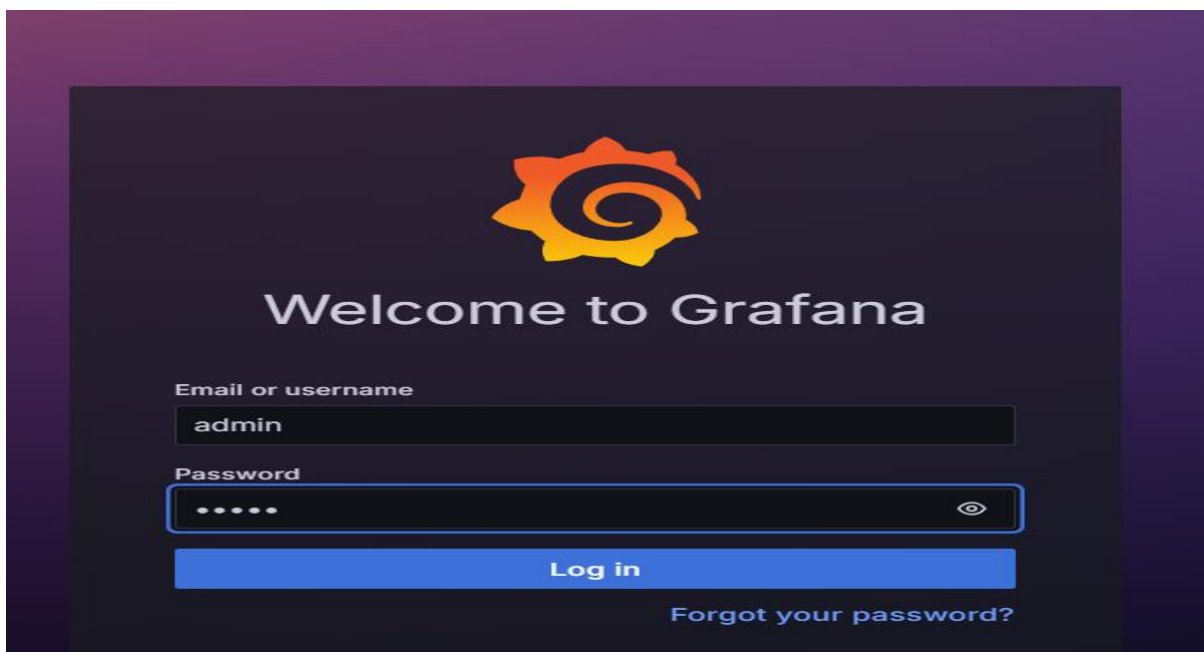
[14. SUDOSYSTEMCTL ENABLE GRAFANA-SERVER](#)

[15. SUDOSYSTEMCTL STATUS GRAFANA-SERVER](#)

- copy your instance's public ip address and place that ip with port range 3000 in your browser .

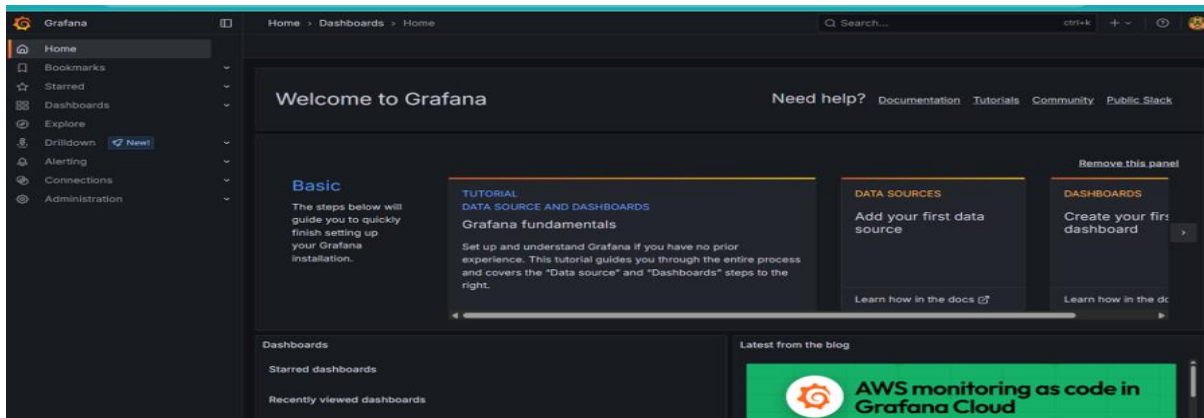
43.204.232.37:3000/login

- After putting ip with port range you'll get this Grafana interface.

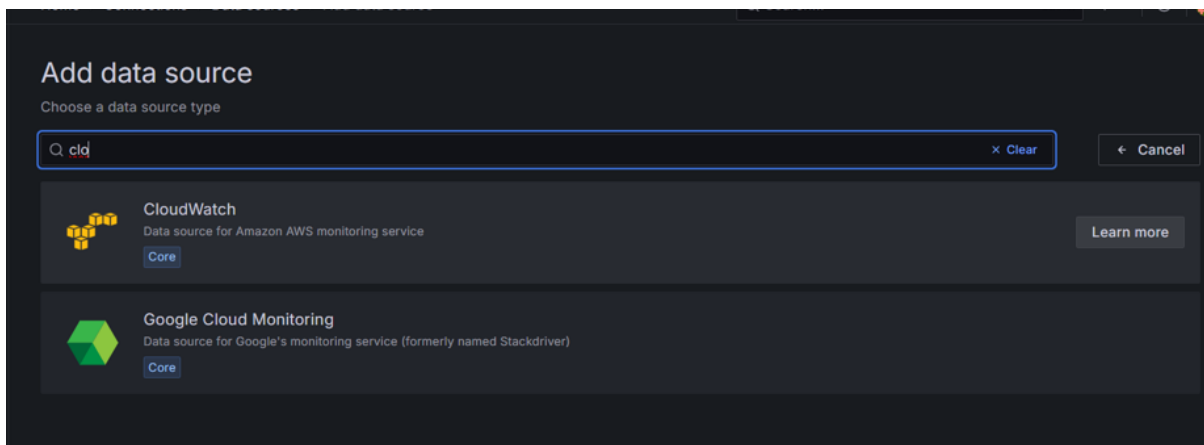


- For making account in Grafana you've to write Admin in "email or username" and "password" both.

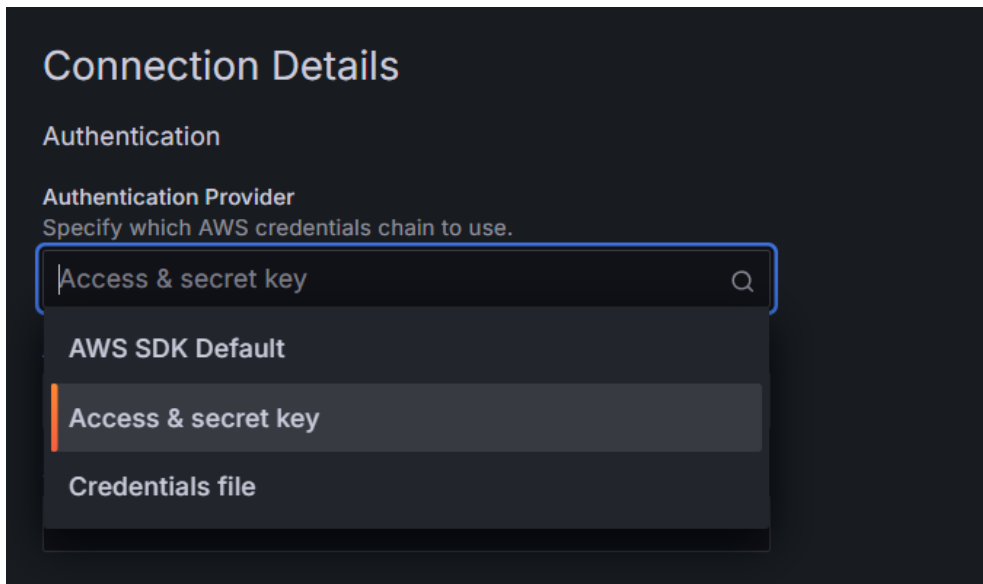
- After this it'll suggest you to create a new password and after that your main Grafana page will be open.



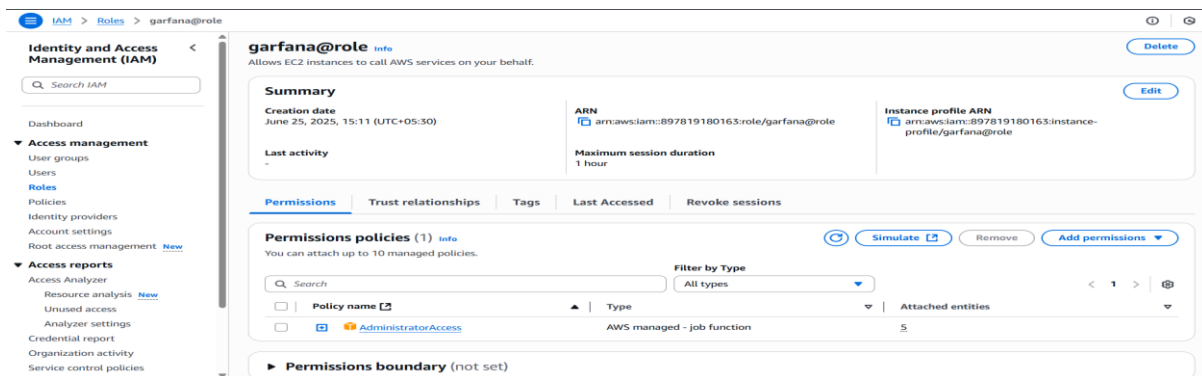
- Now go to connections on the left and data source.
- Click on the add data source.
- Search cloud watch and open it



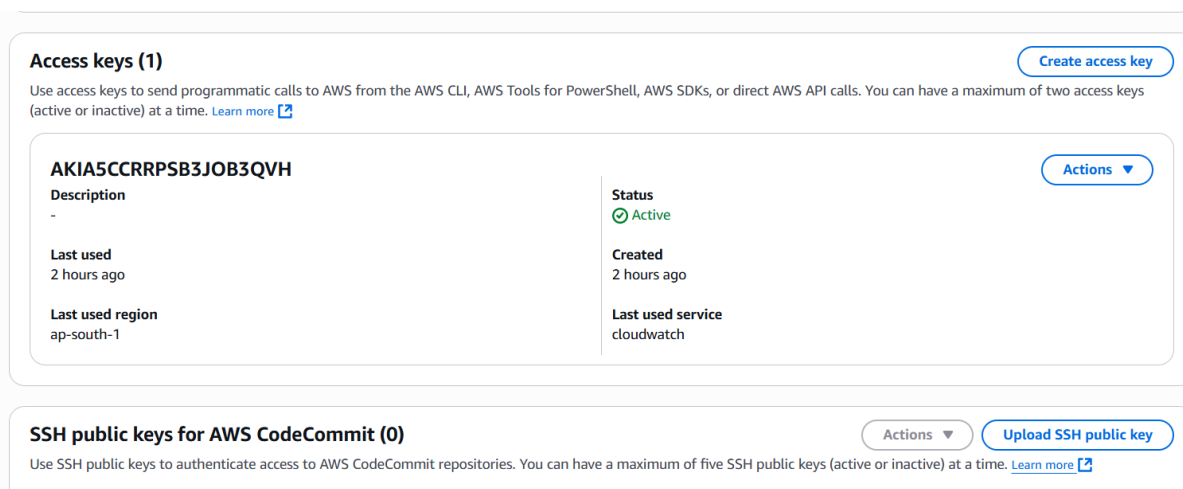
- In connection details:-



- Now go to the IAM if you are a iam user and go to your user id if you are a root user then make your own user.



- Now go to security credentials
- Create on access key



Step 1
Access key best practices & alternatives
 Step 2 - optional
 Set description tag
 Step 3
 Retrieve access keys

Access key best practices & alternatives [Info](#)

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

☒ **Command Line Interface (CLI)**
 You plan to use this access key to enable the AWS CLI to access your AWS account.

☐ **Local code**
 You plan to use this access key to enable application code in a local development environment to access your AWS account.

☐ **Application running on an AWS compute service**
 You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

☐ **Third-party service**
 You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☐ **Application running outside AWS**
 You plan to use this access key to authenticate workloads running in your data center or other

Set description tag - optional [Info](#)

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel

Previous

Create access key

➤ Click on create access key :-

Retrieve access keys [Info](#)

Access key
 If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key | Secret access key

AKIA5CCRRP5BWBYGXIU | ***** [Show](#)

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#) [Done](#)

➤ Now your access key and secret access key is created copy them and paste it and choose region what you choose in the instance

`https://{service}.{region}.amazonaws.com`

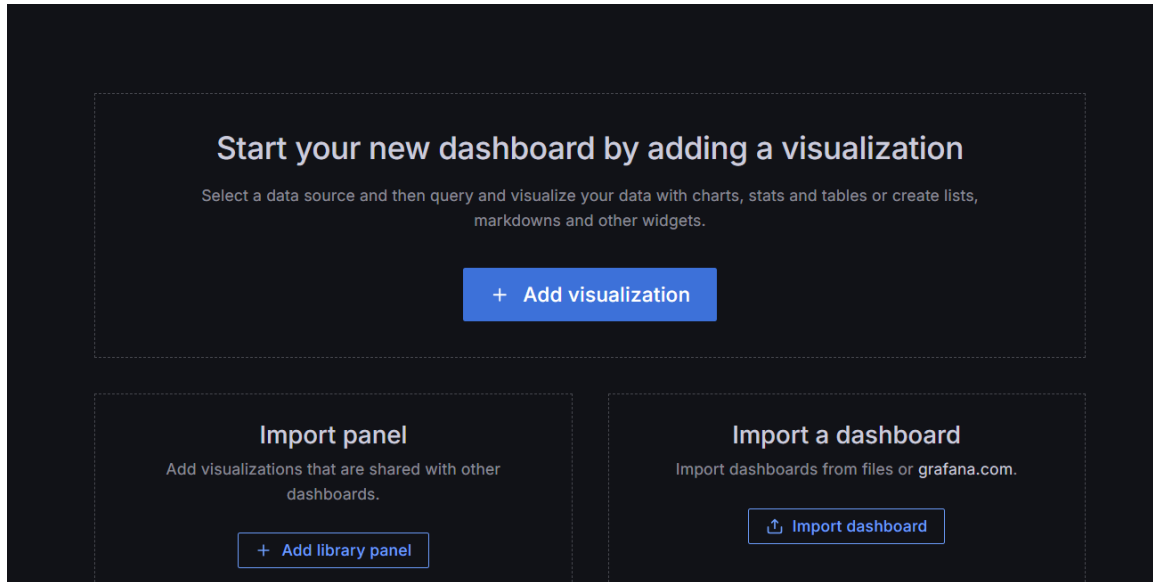
Default Region
 Specify the region, such as for US West (Oregon) use `us-west-2` as the region.

ap-south-1

➤ Now click on save and test:-

✓ 1. Successfully queried the CloudWatch metrics API. 2. Successfully queried the CloudWatch logs API.
Next, you can start to visualize data by [building a dashboard](#), or by querying data in the [Explore view](#).

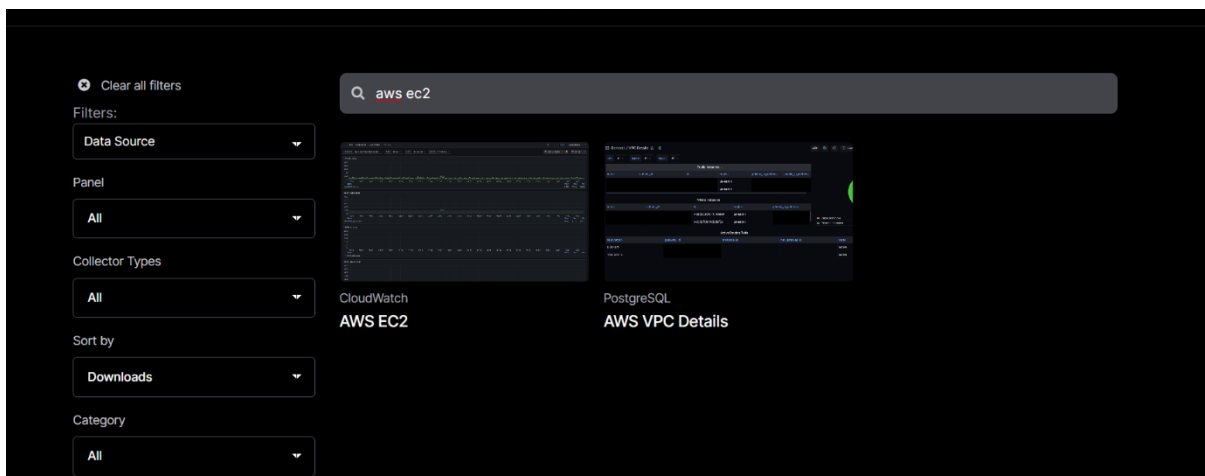
➤ Now next step is we've to go to home and click on dashboard.



➤ Click on import dashboard

Find and import dashboards for common applications at grafana.com/dashboards ↗

- Now click on grafana.com/dashboards
- Search AWS EC2 and open it.



AWS EC2
Visualize AWS EC2 and related EBS metrics

CloudWatch datasource configuration
<http://docs.grafana.org/datasources/cloudwatch/>

Make Grafana AWS dashboards better
Feel free to add additional dashboards for other AWS resources (EC2, S3, ...) or update existing one in [GitHub repo](#).

Commercial support for this dashboard

Monitoring Artist

or
[Download JSON](#)

ID
617

Datasource
CloudWatch

Dependencies
Grafana 11.3.1 Text 5.0.0

Time series 5.0.0

Published by
Monitoring Artist

Last update
2024-12-24T13:47:27

[Edit](#) →

- Now copy the “id number” and place it in dashboard.

Find and import dashboards for common applications at grafana.com/dashboards

617 [Load](#)

And after pasting id number tap on load this interface will appear

Import dashboard
Import dashboard from file or Grafana.com

Importing dashboard from Grafana.com

Published by
Monitoring Artist

Updated on
2024-12-24 19:17:27

Options

Name
AWS EC2

Folder
Dashboards

Unique Identifier (UID)
The unique identifier (UID) of a dashboard can be used for uniquely identify a dashboard between multiple Grafana installs. The UID allows having consistent URLs for accessing dashboards so changing the title of a dashboard will not break any bookmarked links to that dashboard.
AWSEc2000 [Change uid](#)

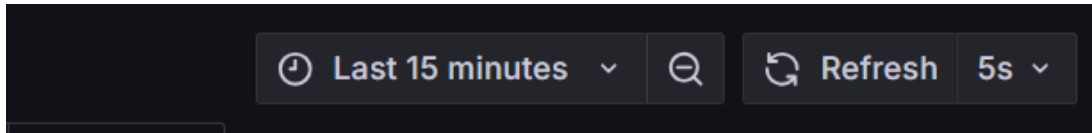
[Import](#) [Cancel](#)

- Now click on import and put cloudwatch in your datasource

Datasource cloudwatch Region default Tag Name All Instance ID i-0571d19f111e75721 Last 24 hours Refresh

EBS volume cloudwatch pe t2.micro

- Region: ap-south1
- Tag-name: your instance name
- Choose refresh time 5 seconds and time last 15 minutes.



➤ Your grafana's interface will appear soon:-

