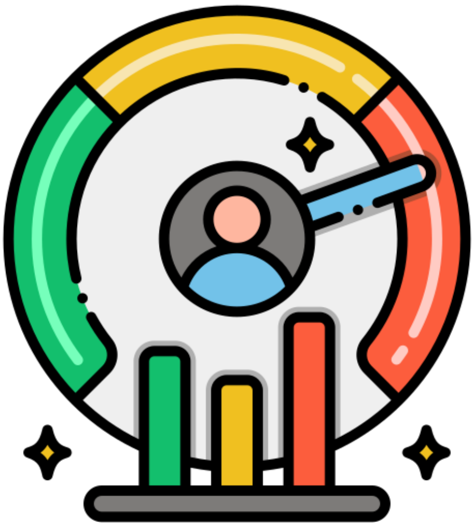


Monitoring High CPU Utilization with Grafana on a Linux Server in AWS

Prepared by: Shavez Khan
BCA 2nd Semester

TABLE OF CONTENTS

1. INTRODUCTION

Effective monitoring and visualization of server performance metrics are essential for maintaining system health and efficiency. This project focuses on integrating Grafana with a Linux server to monitor high CPU utilization.

Grafana is an open-source platform for real-time monitoring and visualization. Prometheus is a monitoring and alerting toolkit optimized for reliability. By combining these tools, we can create a robust solution to monitor and visualize CPU usage, enabling proactive management of server resources.

This project involves setting up an AWS EC2 instance, installing Prometheus and Node Exporter for data collection, configuring Grafana for data visualization, and creating a custom dashboard to track CPU utilization. This integration helps identify performance bottlenecks and ensures efficient resource utilization, providing valuable insights into server performance.

2. GRAFANA

Grafana is an open-source platform for monitoring and visualizing metrics from various data sources. It allows users to create interactive, real-time dashboards that provide insights into system performance, application health, and business metrics.

Key Features:

1. Multi-Source Data Integration: Supports numerous data sources like Prometheus, InfluxDB, Elasticsearch, MySQL, and more.

2. Customizable Dashboards: Offers a wide range of visualizations including graphs, heatmaps, and tables.

3. Real-Time Monitoring: Displays live data and provides alerting capabilities to notify users of important events.

4. User Management: Supports user authentication and role-based access control, making it suitable for team use.

5. Plugins and Extensibility: Allows the addition of new data sources and visualizations through plugins.

6. Open-Source: Benefits from a large community that contributes to its development and support.

Grafana is essential for creating detailed, real-time dashboards that help in proactive system and application monitoring.

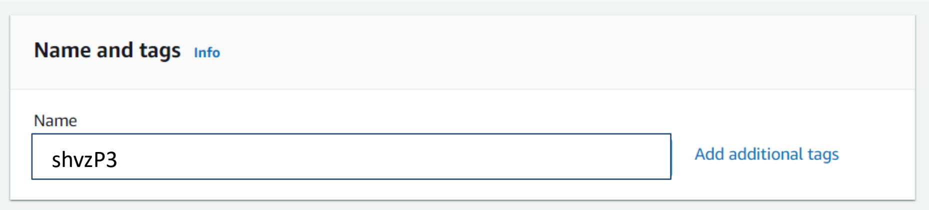
3. STEPS FOR DEPLOYMENT

Step 1:

Set Up AWS EC2 Instance

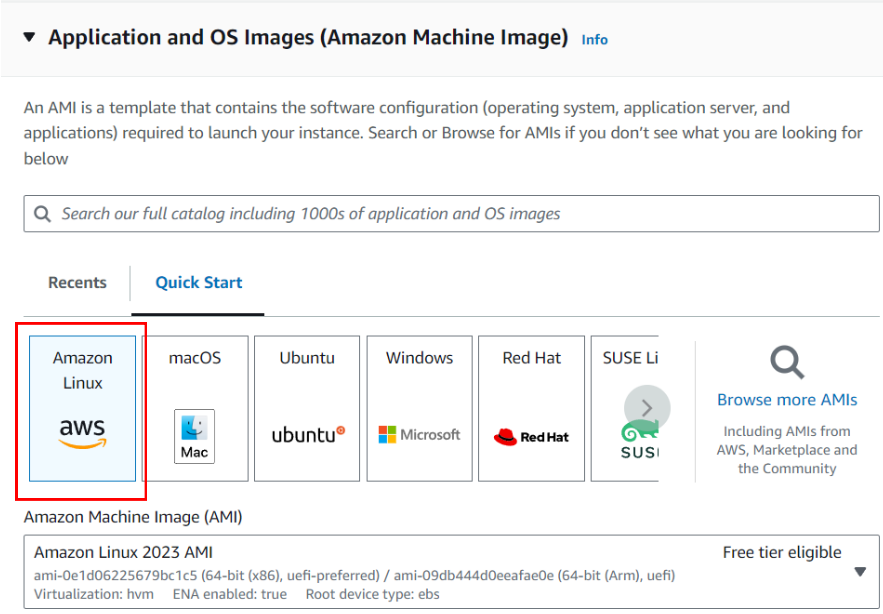
1. Launch an EC2 Instance

- Log in to the AWS Management Console.
- Navigate to the EC2 Dashboard and click "**Launch Instance.**"
- Choose an Amazon Machine Image (AMI), such as **Amazon Linux 2 AMI**.



Name and tags Info

Name: shvzP3



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
Recents
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUSI
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0e1d06225679bc1c5 (64-bit (x86), uefi-preferred) / ami-09db444d0eeafae0e (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

- Select an instance type, such as **t2.micro** (eligible for the free tier).

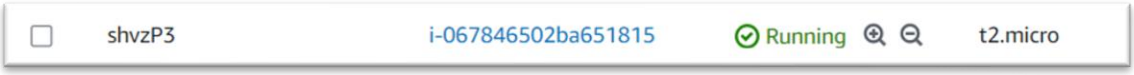
- Create a new keypair **(.ppk)** [for PuTTy]

- Configure instance details, add storage, and configure security group **(allow SSH (port 22) and Grafana (port 3000) ports).**

- Review and launch the instance.

2. Connect to the EC2 Instance

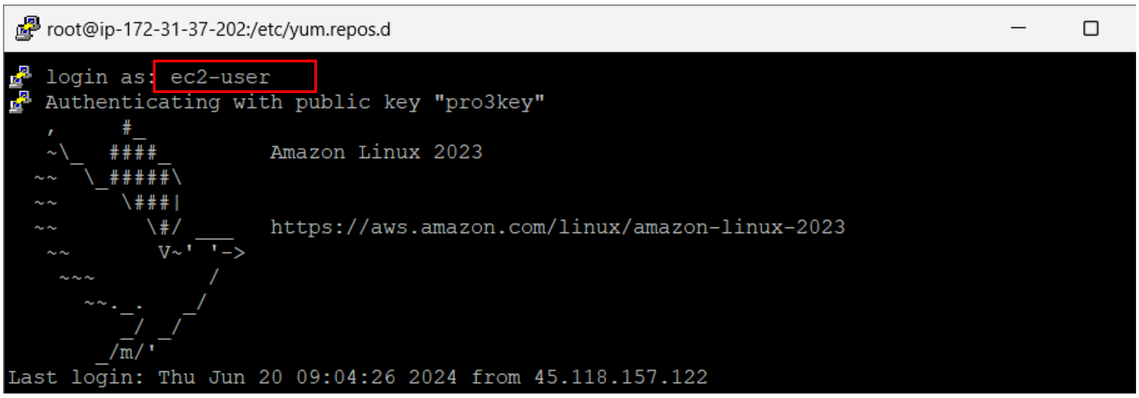
- Click on the instance that you created and copy the *Public IPv4 address*



□	shvzP3	i-067846502ba651815	Running	t2.micro

- Connect to your instance by pasting the address and uploading the key (.ppk) into the PuTTy.

- Type 'ec2-user' and hit Enter to login



root@ip-172-31-37-202:/etc/yum.repos.d

```
login as: ec2-user
Authenticating with public key "pro3key"
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Jun 20 09:04:26 2024 from 45.118.157.122
```

Step 2:

Install Grafana

- Run the following commands

a: Change to Root user: **sudo su**

b: The installation is via yum repository.

Create a **grafana.repo** under **/etc/yum.repos.d/**

vi grafana.repo

c: Put below content in grafana.repo and save it.

```
[grafana]

name=grafana

baseurl=https://packages.grafana.com/oss/rpm

repo_gpgcheck=1

enabled=1

gpgcheck=1

gpgkey=https://packages.grafana.com/gpg.key

sslverify=1


sslcacert=/etc/pki/tls/certs/ca-bundle.crt
```

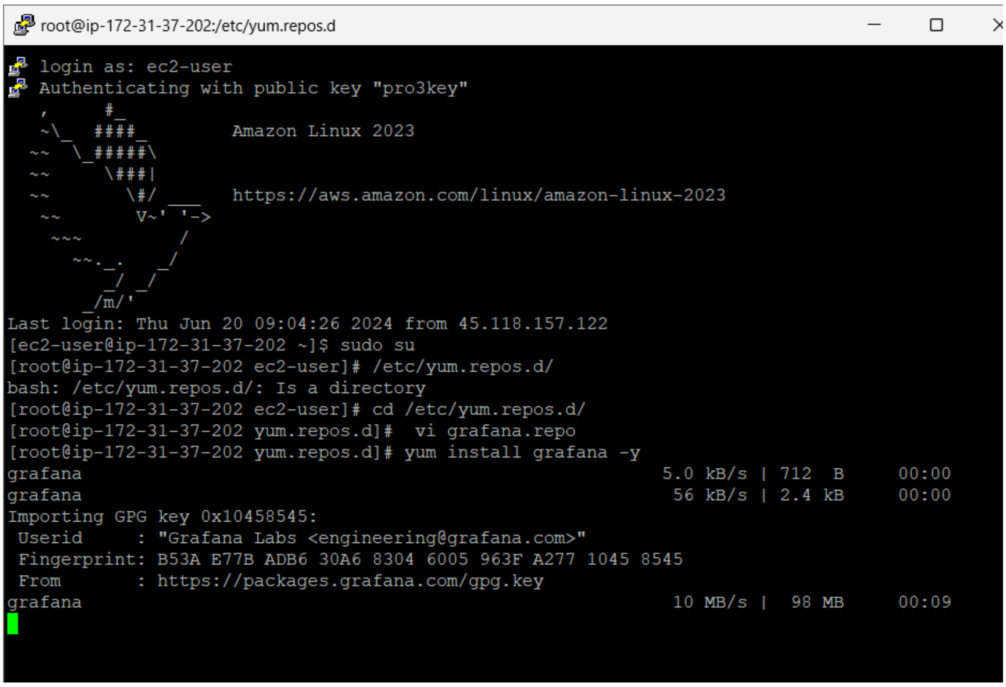
d: Once done with the above steps, It's time to install Grafana.

Type “**sudo yum -y install Grafana**”

e: Start the server -

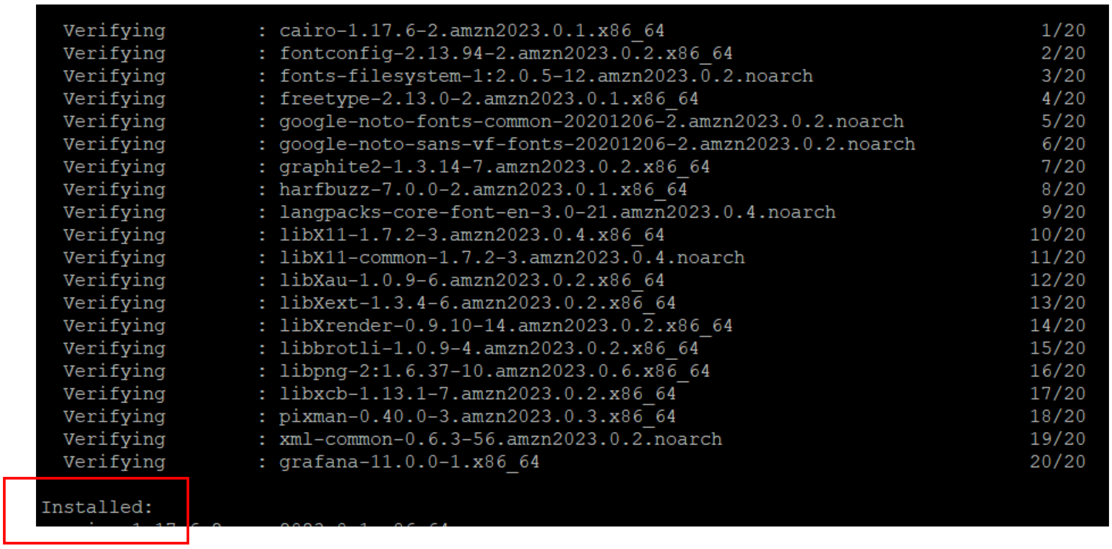
systemctl start grafana-server

systemctl status grafana-server



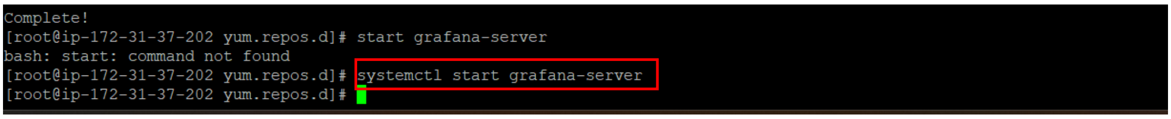
root@ip-172-31-37-202:/etc/yum.repos.d

```
login as: ec2-user
Authenticating with public key "pro3key"
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Thu Jun 20 09:04:26 2024 from 45.118.157.122
[ec2-user@ip-172-31-37-202 ~]$ sudo su
[root@ip-172-31-37-202 ec2-user]# /etc/yum.repos.d/
bash: /etc/yum.repos.d/: Is a directory
[root@ip-172-31-37-202 ec2-user]# cd /etc/yum.repos.d/
[root@ip-172-31-37-202 yum.repos.d]#  vi grafana.repo
[root@ip-172-31-37-202 yum.repos.d]# yum install grafana -y
grafana                                                 5.0 kB/s | 712  B     00:00
grafana                                                  56 kB/s | 2.4 kB     00:00
Importing GPG key 0x10458545:
 Userid     : "Grafana Labs <engineering@grafana.com>"
 Fingerprint: B53A E77B ADB6 30A6 8304 6005 963F A277 1045 8545
 From       : https://packages.grafana.com/gpg.key
grafana                                                  10 MB/s |  98 MB     00:09
```



```
  Verifying        : cairo-1.17.6-2.amzn2023.0.1.x86_64                      1/20
  Verifying        : fontconfig-2.13.94-2.amzn2023.0.2.x86_64                2/20
  Verifying        : fonts-filesystem-1:2.0.5-12.amzn2023.0.2.noarch         3/20
  Verifying        : freetype-2.13.0-2.amzn2023.0.1.x86_64                   4/20
  Verifying        : google-noto-fonts-common-20201206-2.amzn2023.0.2.noarch 5/20
  Verifying        : google-noto-sans-vf-fonts-20201206-2.amzn2023.0.2.noarch 6/20
  Verifying        : graphite2-1.3.14-7.amzn2023.0.2.x86_64                  7/20
  Verifying        : harfbuzz-7.0.0-2.amzn2023.0.1.x86_64                    8/20
  Verifying        : langpacks-core-font-en-3.0-21.amzn2023.0.4.noarch       9/20
  Verifying        : libX11-1.7.2-3.amzn2023.0.4.x86_64                     10/20
  Verifying        : libX11-common-1.7.2-3.amzn2023.0.4.noarch              11/20
  Verifying        : libXau-1.0.9-6.amzn2023.0.2.x86_64                     12/20
  Verifying        : libXext-1.3.4-6.amzn2023.0.2.x86_64                    13/20
  Verifying        : libXrender-0.9.10-14.amzn2023.0.2.x86_64               14/20
  Verifying        : libbrotli-1.0.9-4.amzn2023.0.2.x86_64                  15/20
  Verifying        : libpng-2:1.6.37-10.amzn2023.0.6.x86_64                 16/20
  Verifying        : libxcb-1.13.1-7.amzn2023.0.2.x86_64                    17/20
  Verifying        : pixman-0.40.0-3.amzn2023.0.3.x86_64                    18/20
  Verifying        : xml-common-0.6.3-56.amzn2023.0.2.noarch                19/20
  Verifying        : grafana-11.0.0-1.x86_64                                20/20

Installed:
```



```
Complete!
[root@ip-172-31-37-202 yum.repos.d]# start grafana-server
bash: start: command not found
[root@ip-172-31-37-202 yum.repos.d]# systemctl start grafana-server
[root@ip-172-31-37-202 yum.repos.d]#
```

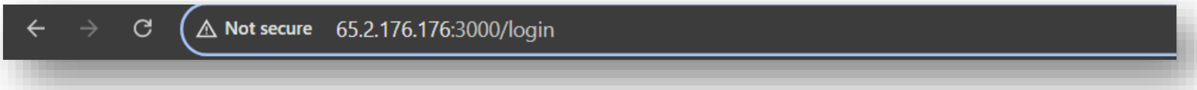
Grafana is successfully installed !!!

Step 3:

Login to Grafana

- Copy your instance's *Public iPv4 address* and add **:300/login**

  Ex- 65.2.176.176 → 65.2.176.176:300/login

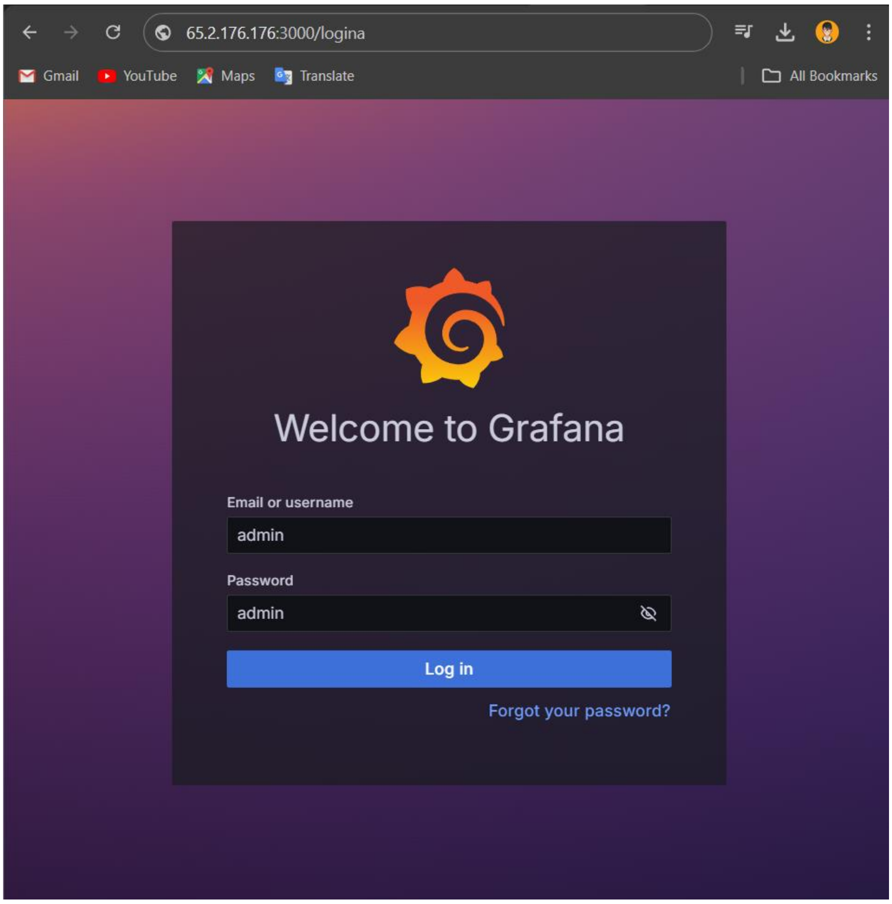


Not secure 65.2.176.176:3000/login

- Hit the enter button and you'll be redirected to the Grafana Login page

Userame: **admin**

Password: **admin**



Email or username: admin

Password: admin

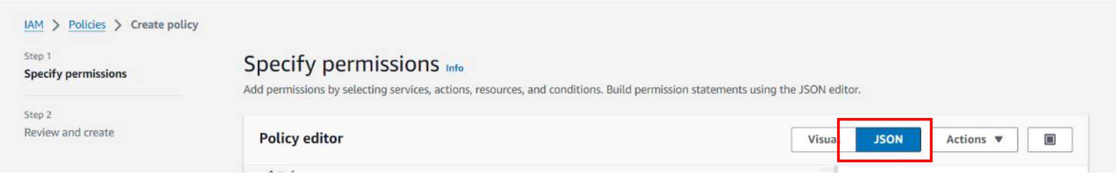
- After login, you can change the username and password

Prepared by: Shavez Khan
BCA 2nd Semester

Step 4:

Create a policy for EC2 instance

- Go to **IAM > Policies > Create policy**



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

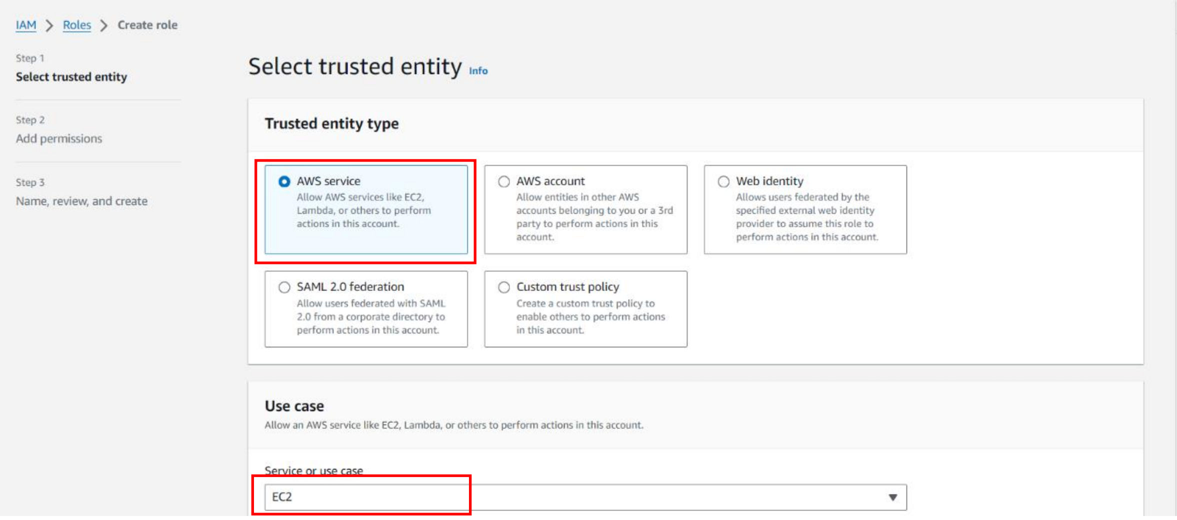
- Click on **JSON** and paste the Policy given below

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "VisualEditor0",
                        "Effect": "Allow",
                        "Action": [
                                "ec2:DescribeInstances",
                                "cloudwatch:GetMetricData",
                                "ec2:DescribeTags",
                                "ec2:DescribeRegions",
                                "cloudwatch:GetMetricStatistics",
                                "cloudwatch:ListMetrics"
                        ],
                        "Resource": "*"
                },
    {
      "Sid": "AllowReadingTagsInstancesRegionsFromEC2",
      "Effect":"Allow",
      "Action": ["ec2:DescribeTags","ec2:DescribeInstances","ec2:DescribeRegions"],
      "Resource":"*"
    },
    {
      "Sid": "AllowReadingResoucesForTags",
      "Effect":"Allow",
      "Action":"tag:GetResources",
      "Resource":"*"
    }
        ]
}
```

- Give a **name** to your policy and **save it.**

Now attach this policy to a Role and to do this we need to create a role and attach this policy to it.

- Go to **IAM > Role > Create role**



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

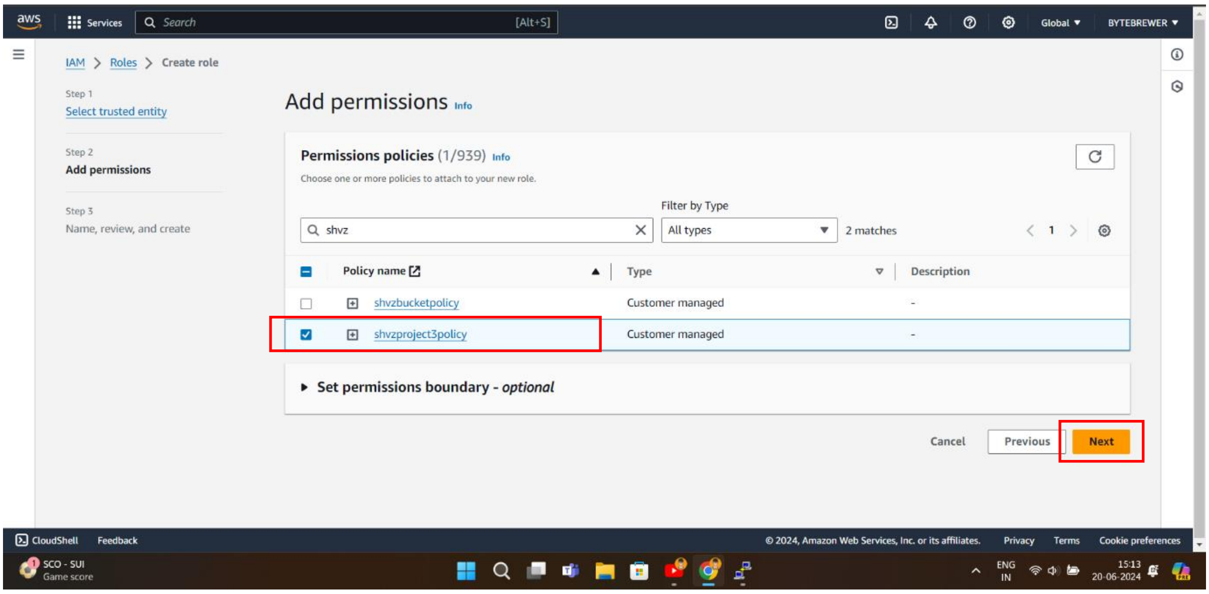
○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

- **Attach the Policy that we created**



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (1/939) Info
Choose one or more policies to attach to your new role.

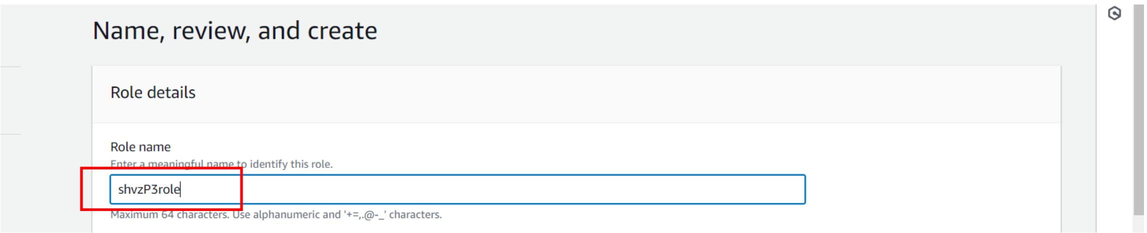
Filter by Type

shvz | All types | 2 matches

	Policy name	Type	Description
□	shvzbucketpolicy	Customer managed	-
☑	shvzproject3policy	Customer managed	-

▸ **Set permissions boundary - *optional***

- **Give a name to the role and hit Create role button**



Name, review, and create

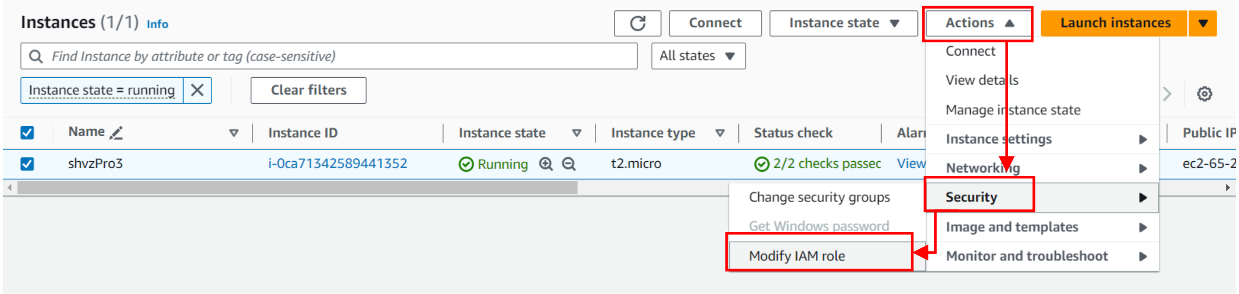
Role details

Role name
Enter a meaningful name to identify this role.
shvzP3role
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Prepared by: Shavez Khan
BCA 2nd Semester

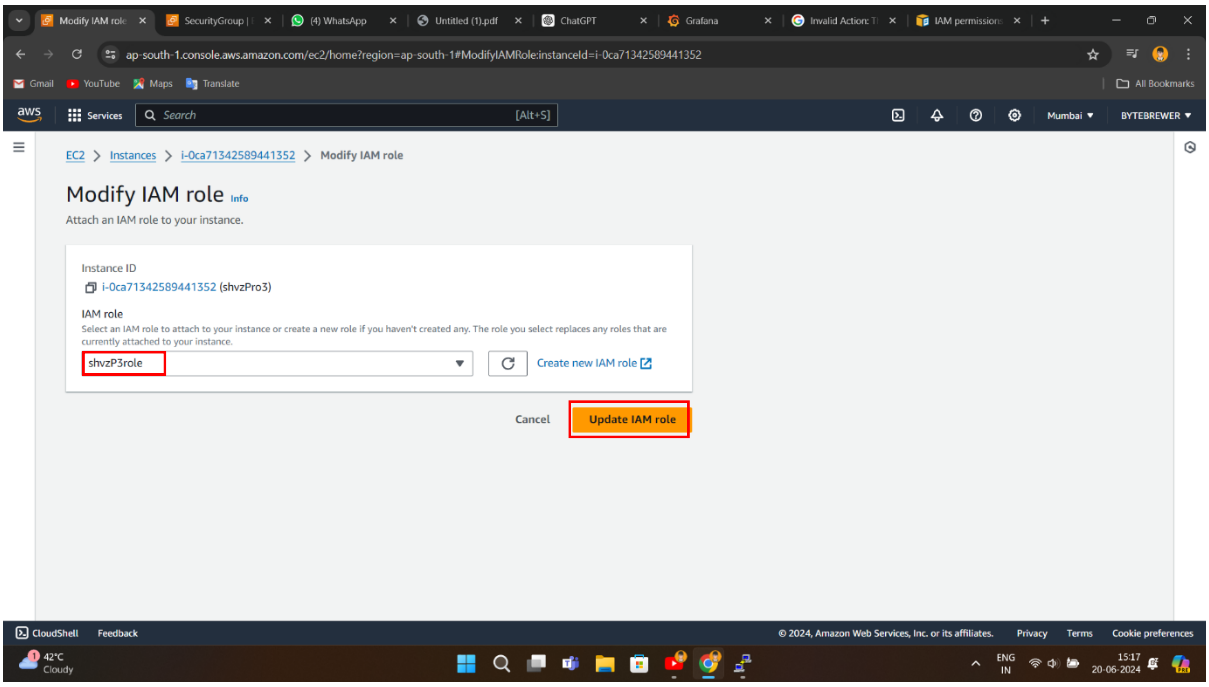
Now go to instances tab and Modify IAM Role, to do this –

- *Select your instance **> ACTIONS > Security > Modify IAM role***



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm	Public IP
☑	shvzPro3	i-0ca71342589441352	Running	t2.micro	2/2 checks passed	View	ec2-65-2

- *Select the role we created and click on **<u>Update IAM role</u>***



Modify IAM role Info

Attach an IAM role to your instance.

Instance ID

i-0ca71342589441352 (shvzPro3)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

shvzP3role ▼

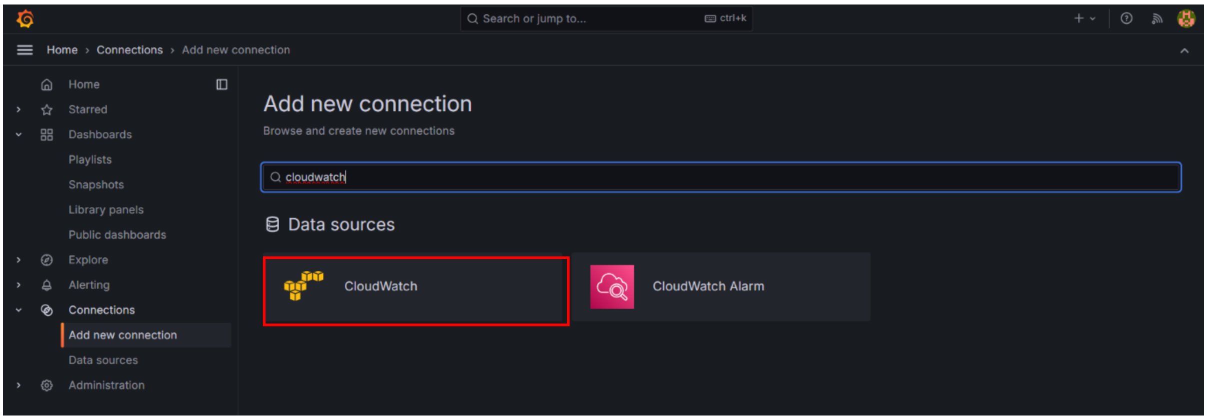
All set, now we have add new connection (CLOUDWATCH) to Grafana and add dashboards

Step 5:

Set-Up Grafana

We need to add a new connection to Grafana using Cloudwatch so that it can display the monitoring data. To do this –

- *Go To **Grafana** > **Home** > **Connections** > **Add new connections >** **Cloudwatch** (search it)*



Home › Connections › Add new connection

Add new connection

Browse and create new connections

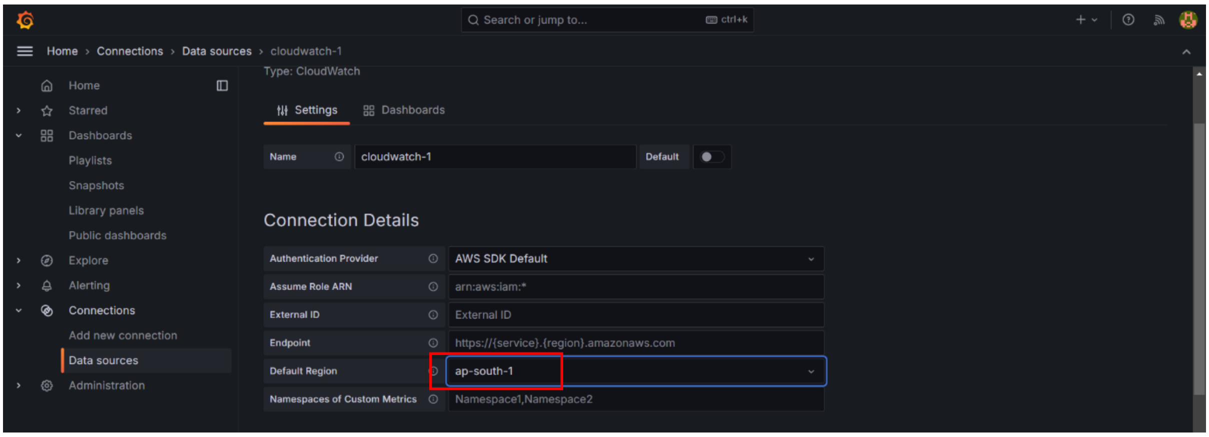
cloudwatch

Data sources

CloudWatch

CloudWatch Alarm

- **In Settings** > choose the region **ap-south-1 > Save/Test**



Home › Connections › Data sources › cloudwatch-1

Type: CloudWatch

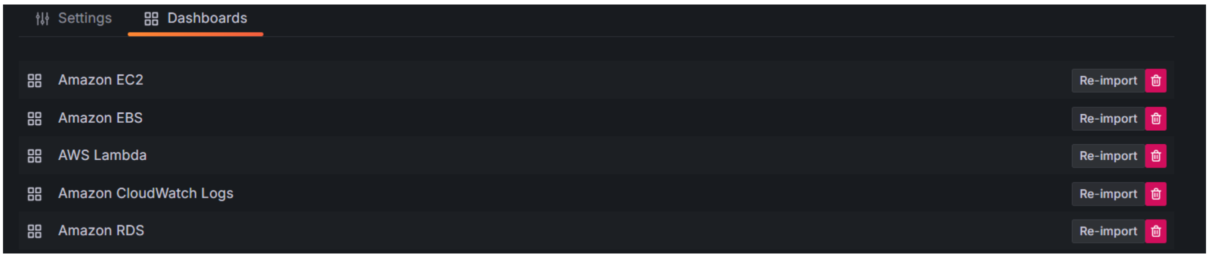
Settings | Dashboards

Name: cloudwatch-1 | Default

Connection Details

Authentication Provider	AWS SDK Default
Assume Role ARN	arn:aws:iam:*
External ID	External ID
Endpoint	https://{service}.{region}.amazonaws.com
Default Region	ap-south-1
Namespaces of Custom Metrics	Namespace1,Namespace2

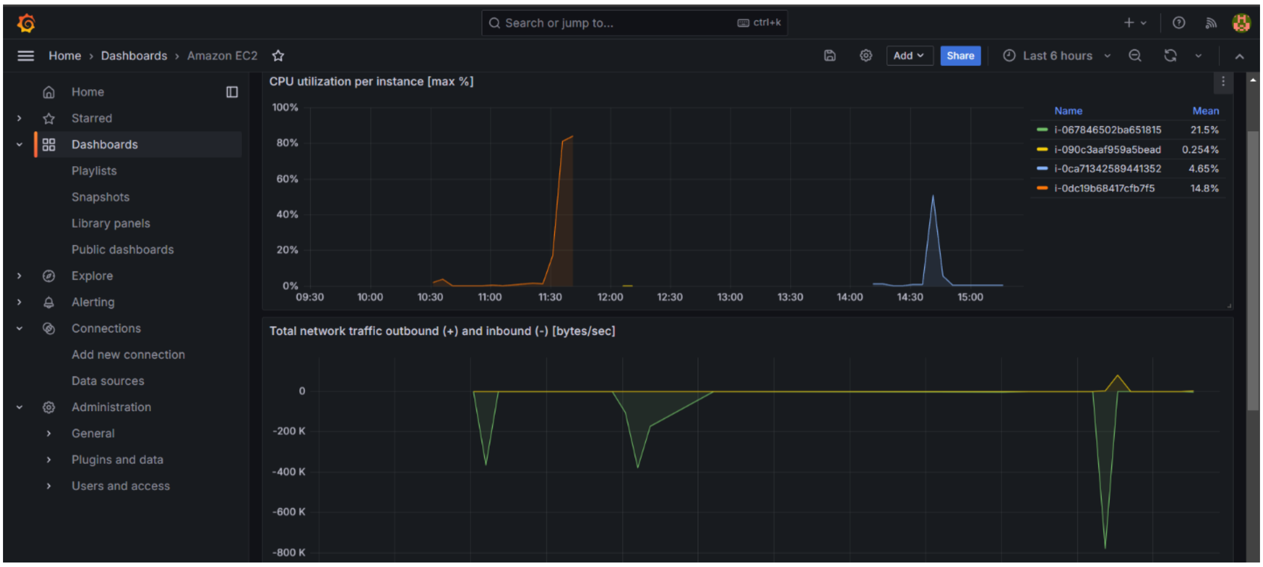
- **Dashboards** > import the dashboards



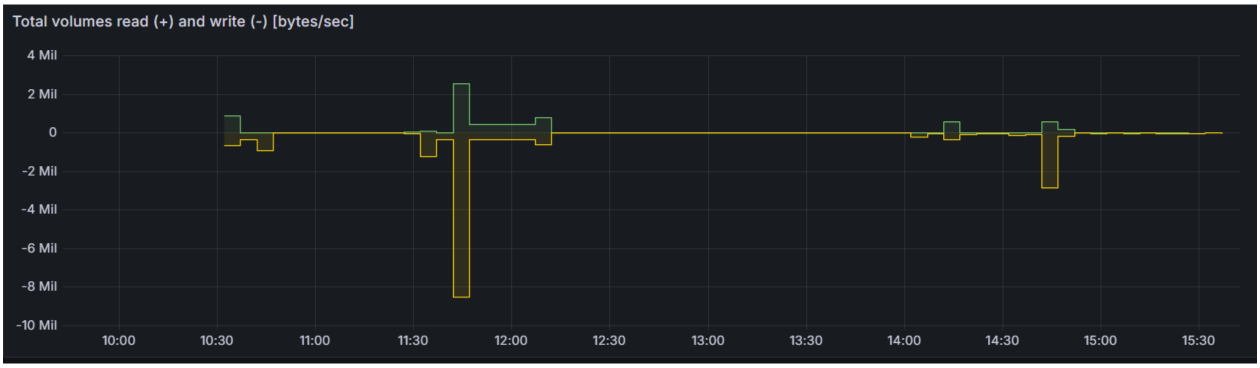
Settings | Dashboards

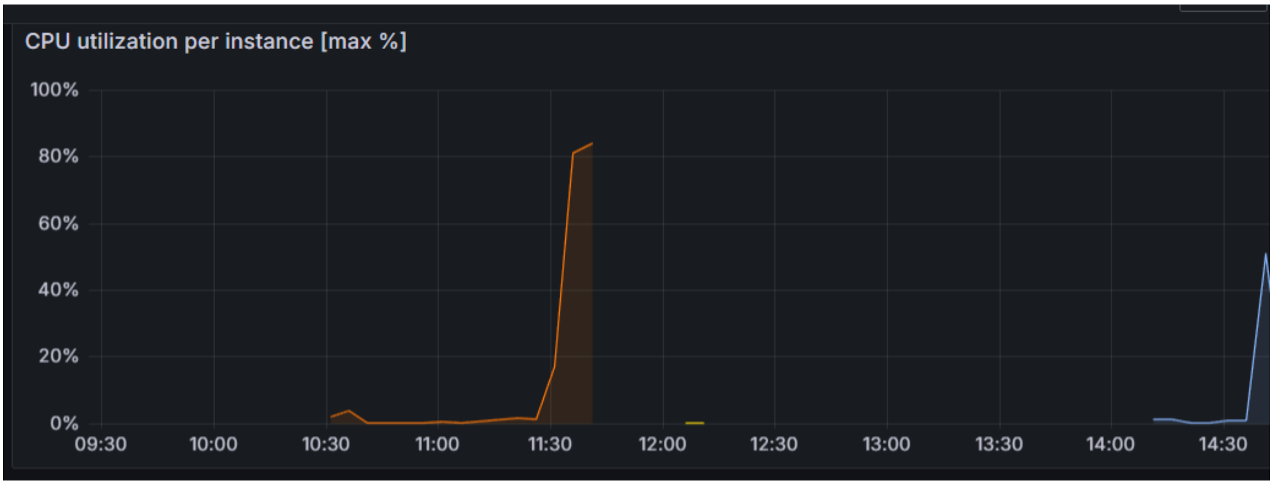
Amazon EC2	Re-import
Amazon EBS	Re-import
AWS Lambda	Re-import
Amazon CloudWatch Logs	Re-import
Amazon RDS	Re-import

Now check the Dashboard



	Name	Mean
🟩	i-067846502ba651815	21.5%
🟨	i-090c3aaf959a5bead	0.254%
🟦	i-0ca71342589441352	4.65%
🟧	i-0dc19b68417cfb7f5	14.8%





4. CONCLUSION

In this project, we successfully integrated Grafana with a Linux server and connected it to AWS Cloudwatch to monitor high CPU utilization and other critical metrics. By following the detailed steps provided, we configured Grafana to visualize performance data from Cloudwatch, enabling comprehensive and real-time monitoring of our server and AWS resources. This setup enhances our ability to manage and optimize system performance proactively, leveraging the power of Grafana's visualization capabilities combined with AWS Cloudwatch's robust monitoring features.

This integration demonstrates the efficiency and effectiveness of using Grafana and Cloudwatch for robust infrastructure monitoring and management.

5. REFERENCES

- Grafana
- Amazon Managed Grafana