

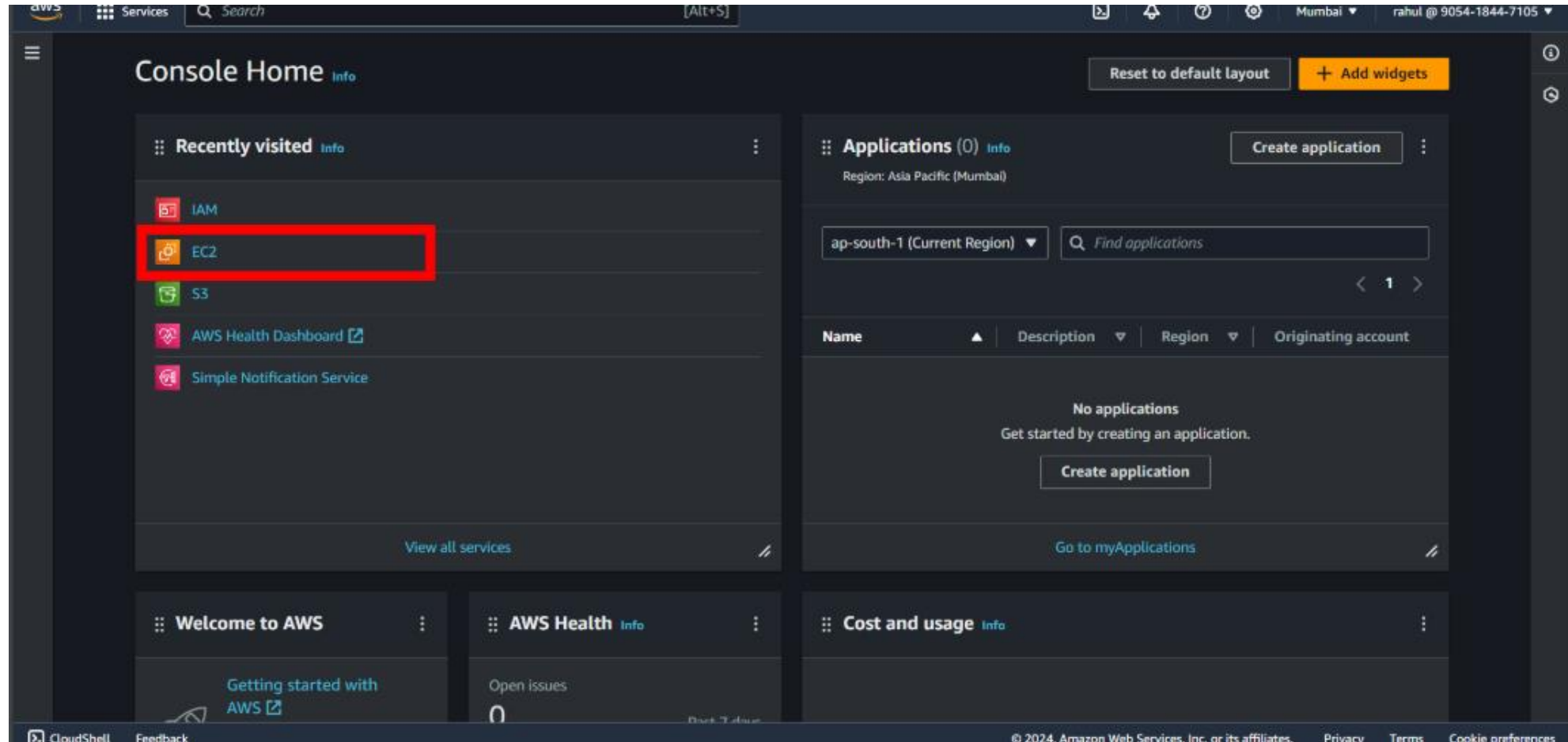
INDEX:

Serial number	Name of topic
1.	Sign in to AWS Management Console:
2.	Create an EC2 Instance:
3.	Installation of GRAFANA into instance:
4.	Creating policy:
5.	Creating role :
6.	Modifying security rules:
7.	Starting GRAFANA:
8.	Adding data source to grafana :
9.	Graph of CPU utilization in GRAFANA :

Sign in to AWS Management Console:

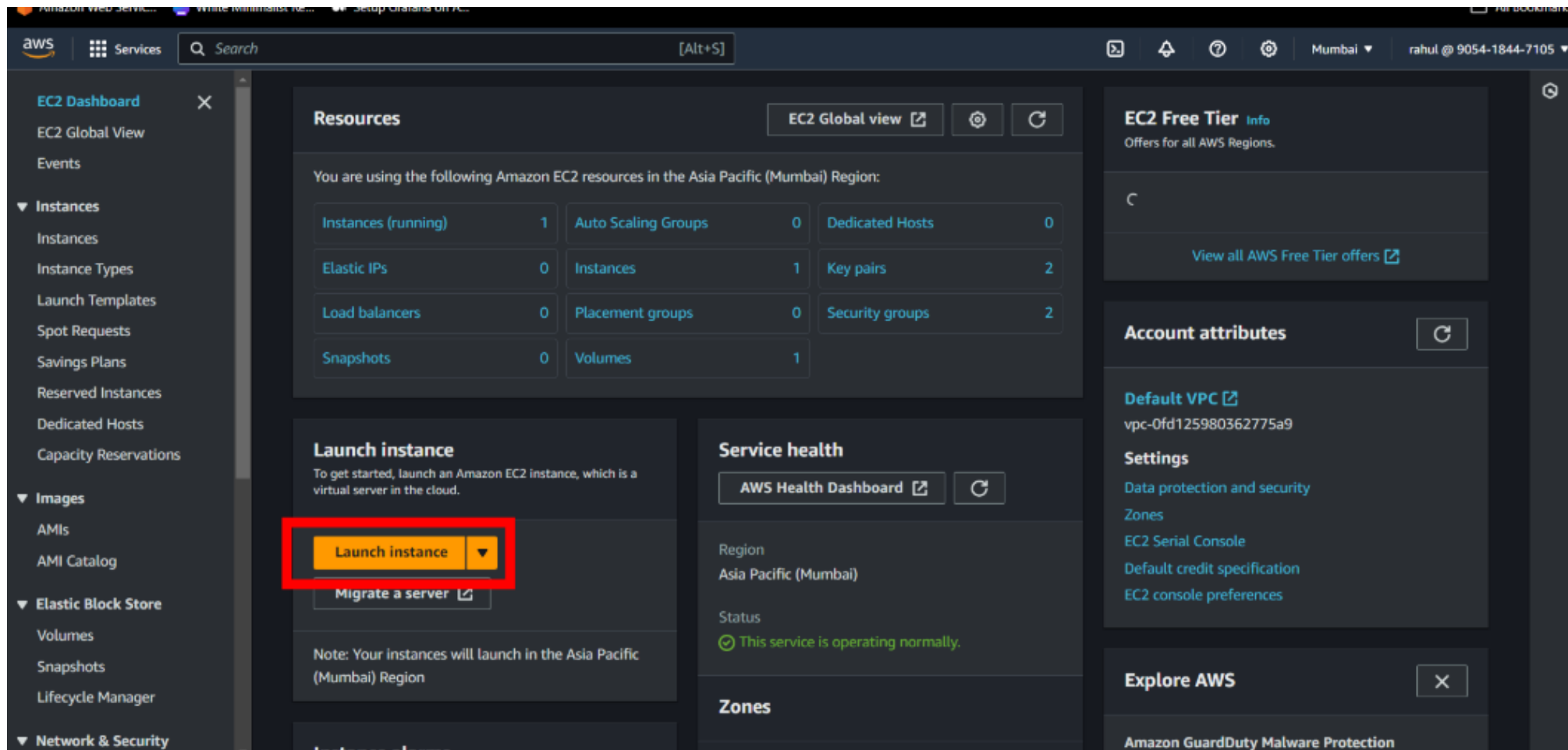
-
1. Click on the Open Console button, and you will get redirected to AWS Console in a new browser tab.
 - On the AWS sign-in page, Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
 - Now copy your User Name and Password in the Lab Console to the IAM Username and Password in AWS Console and click on the Sign in button.

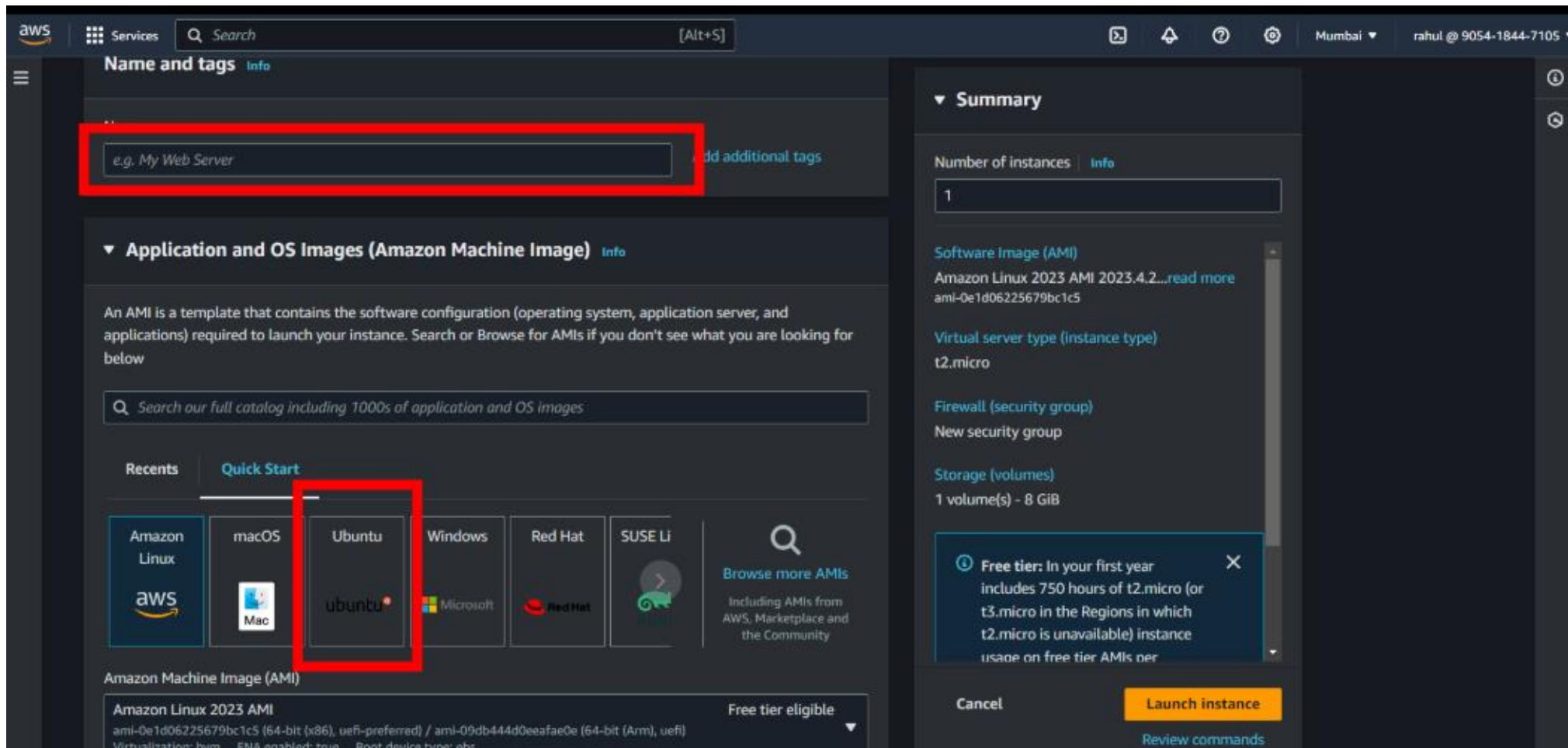
2. Once Signed in to the AWS Management Console, Make the default AWS Region as US East (N. Virginia) us-east-1.



❖ Create an EC2 Instance(ubuntu):

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





- Provide the EC2 name of your choice and select "**Ubuntu**" as an OS Image.

The screenshot displays the AWS Management Console interface for creating a new instance. The left sidebar shows the navigation menu with 'Instance type' selected. The main content area is divided into two columns. The left column contains the 'Instance type' section, which shows 't2.micro' as the selected instance type. Below this, the 'Key pair (login)' section is highlighted with a red box, and the 'Create new key pair' link is also highlighted with a red box. The right column contains the 'Summary' section, which shows the configuration details for the instance, including the number of instances (1), the software image (Amazon Linux 2023 AMI), the virtual server type (t2.micro), the firewall (security group), and the storage (volumes). A 'Free tier' notification is visible at the bottom right of the console.

Instance type Info | Get advice

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.0124 USD per Hour

On-Demand Windows base pricing: 0.017 USD per Hour

On-Demand RHEL base pricing: 0.0724 USD per Hour

On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select

Create new key pair

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.4.2...read more

ami-0e1d06225679bc1c5

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per

Cancel Launch instance

Review commands

- Create a new key pair.

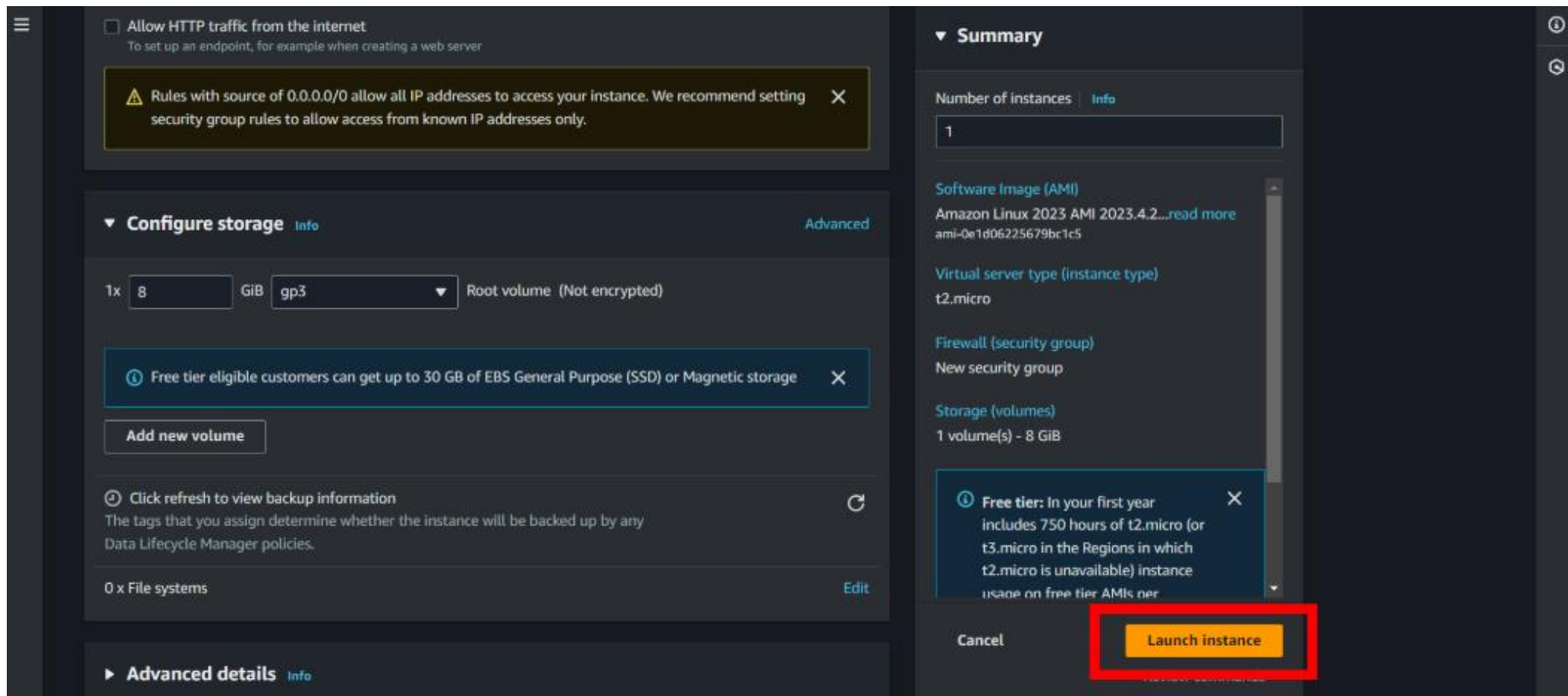
The screenshot displays the AWS Management Console interface for launching an EC2 instance. A modal dialog titled "Create key pair" is open, requiring the following information:

- Key pair name:** grafana2
- Key pair type:** RSA (selected), ED25519
- Private key file format:** .pem, .ppk (selected)

A warning message states: "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." Buttons for "Cancel" and "Create key pair" are at the bottom of the dialog.

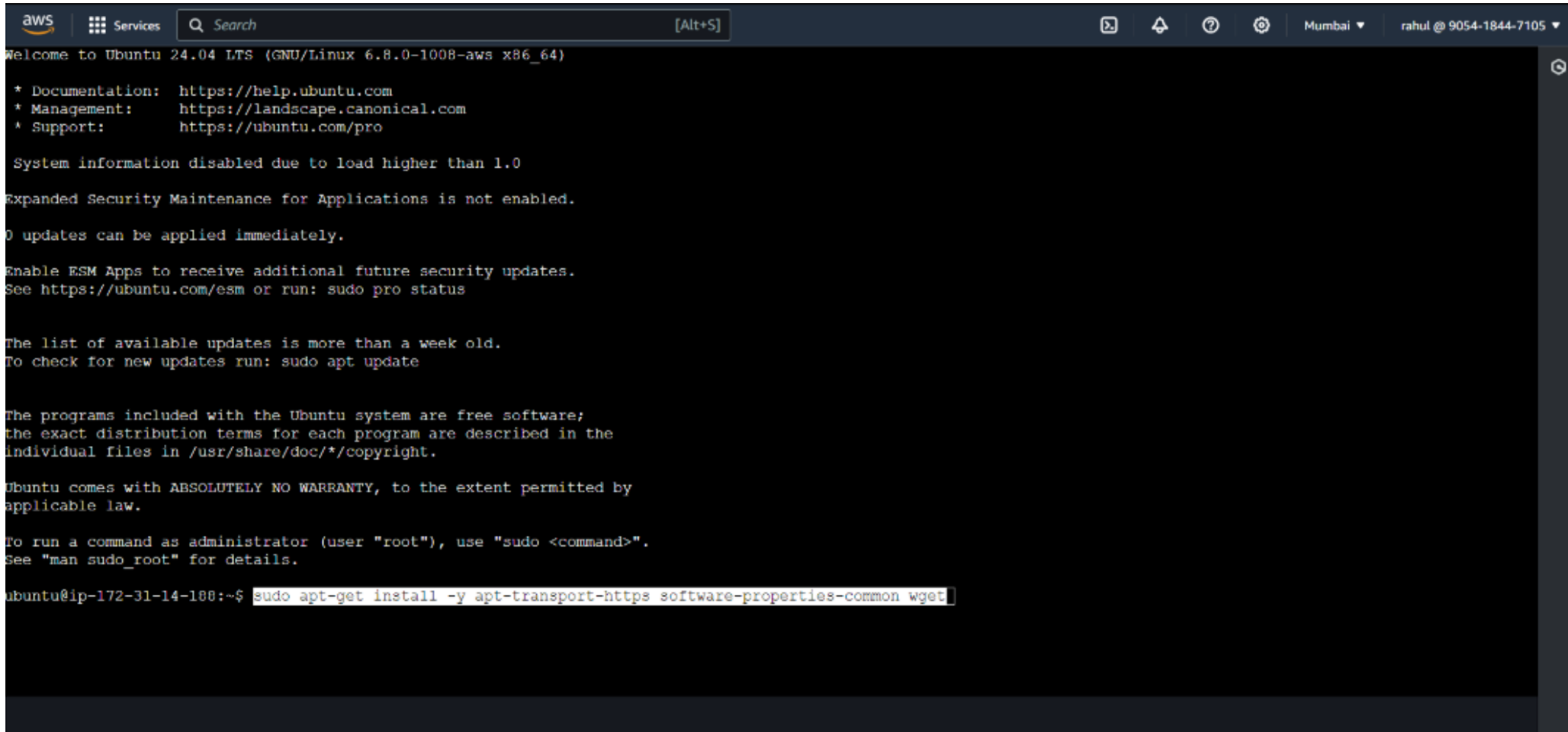
In the background, the "Launch an instance" page is visible, showing the "Instance type" section with details for the t2.micro instance (1 vCPU, 1 GiB Memory) and pricing information. Other sections like "Key pair (login)", "Network settings", and "Summary" are also partially visible.

- Scroll down and click on “LAUNCH 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.

❖ Installation of GRAFANA into instance:



```
aws Services Search [Alt+S] Mumbai rahul @ 9054-1844-7105
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

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

System information disabled due to load higher than 1.0

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

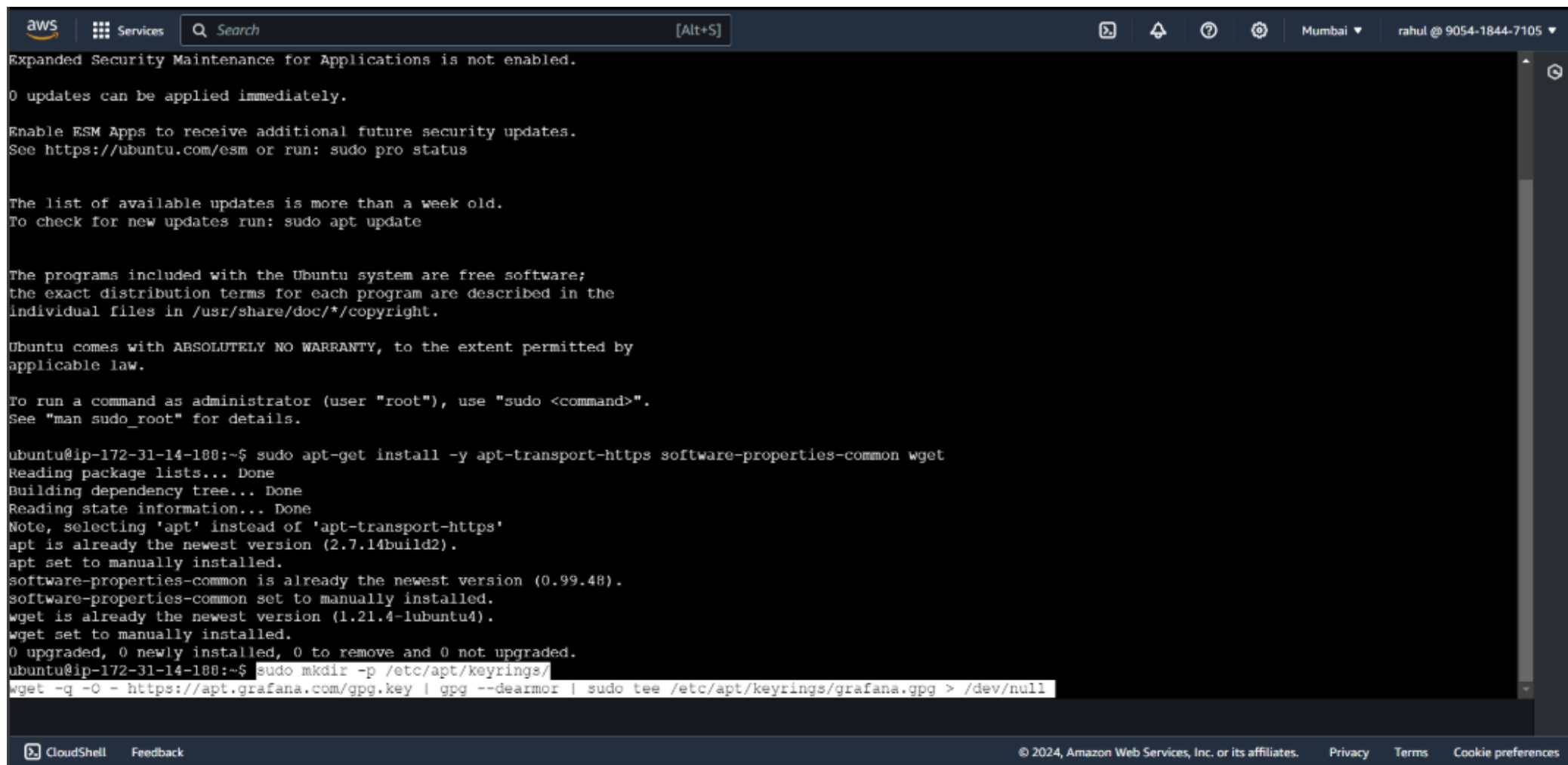
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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-172-31-14-188:~$ sudo apt-get install -y apt-transport-https software-properties-common wget
```

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



The screenshot shows an AWS CloudShell terminal window. The top bar includes the AWS logo, 'Services', a search bar, and user information 'Mumbai' and 'rahul @ 9054-1844-7105'. The terminal output displays system messages about security updates and the Ubuntu license. The user then runs a command to install 'apt-transport-https', 'software-properties-common', and 'wget'. The output shows that 'apt' and 'software-properties-common' are already installed, while 'wget' is updated. Finally, the user runs a command to create a GPG keyring for Grafana by downloading a key from the Grafana website and adding it to the keyring.

```
aws Services Search [Alt+S] Mumbai rahul @ 9054-1844-7105

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-172-31-14-180:~$ 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'
apt is already the newest version (2.7.14build2).
apt set to manually installed.
software-properties-common is already the newest version (0.99.48).
software-properties-common set to manually installed.
wget is already the newest version (1.21.4-lubuntu4).
wget set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-14-180:~$ 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
```

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

*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*

```
aws Services Search [Alt+S] Mumbai rahul @ 9054-1844-7105
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

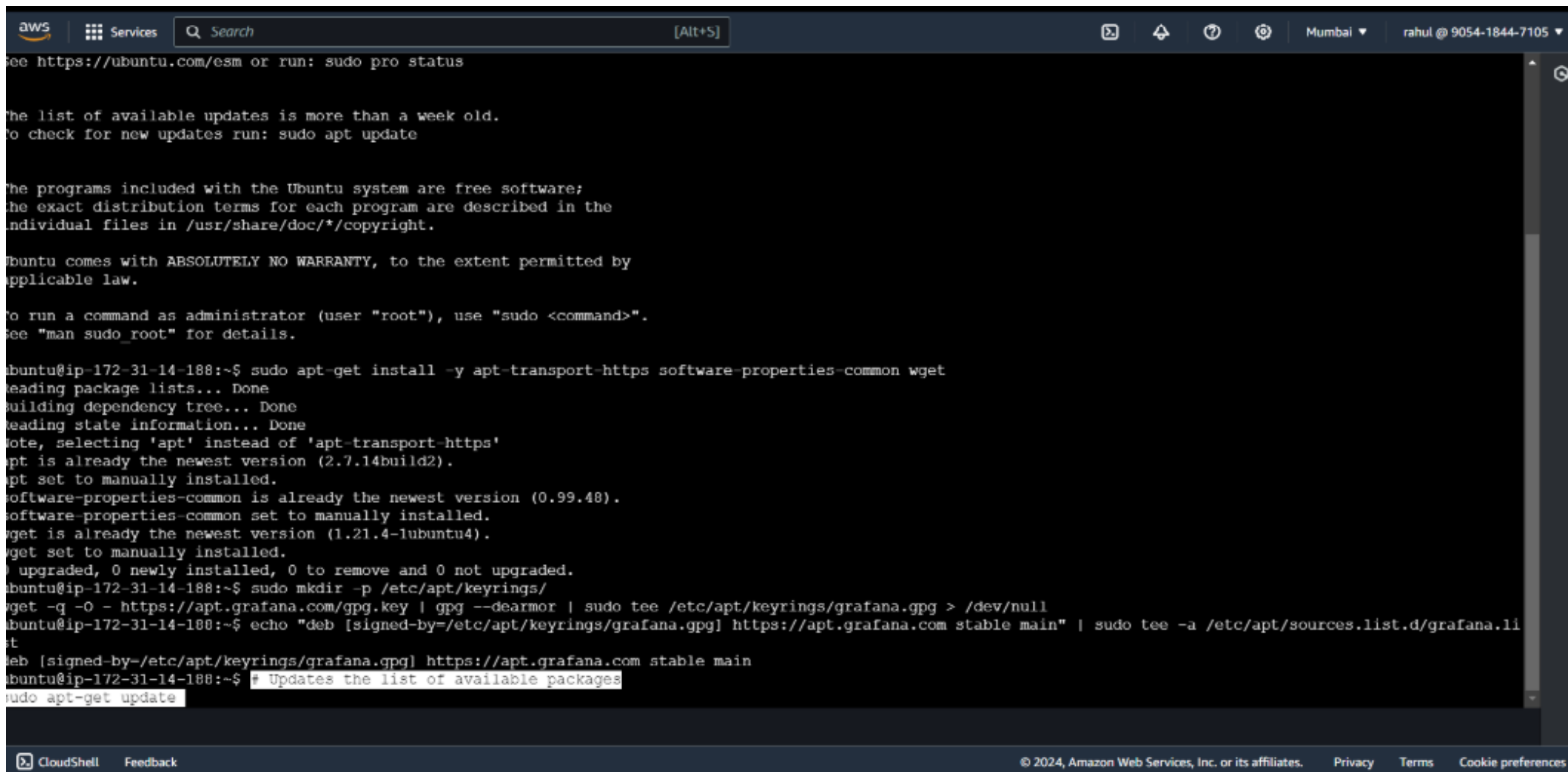
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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-172-31-14-188:~$ 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'
apt is already the newest version (2.7.14build2).
apt set to manually installed.
software-properties-common is already the newest version (0.99.48).
software-properties-common set to manually installed.
wget is already the newest version (1.21.4-1ubuntu4).
wget set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-14-188:~$ 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
ubuntu@ip-172-31-14-188:~$ echo "deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.li
st
```

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



```
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-172-31-14-188:~$ 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'
apt is already the newest version (2.7.14build2).
apt set to manually installed.
software-properties-common is already the newest version (0.99.40).
software-properties-common set to manually installed.
wget is already the newest version (1.21.4-1ubuntu4).
wget set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-14-188:~$ 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
ubuntu@ip-172-31-14-188:~$ 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
deb [signed-by=/etc/apt/keyrings/grafana.gpg] https://apt.grafana.com stable main
ubuntu@ip-172-31-14-188:~$ # Updates the list of available packages
sudo apt-get update
```

To updates the list of available packages
sudo apt-get update

```
aws Services Search [Alt+S] Mumbai rahul@9054-1844-7105
Get:22 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [25.1 kB]
Get:23 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [112 B]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [70.1 kB]
Get:26 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [14.3 kB]
Get:27 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:28 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [2968 B]
Get:29 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [968 B]
Get:30 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:31 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [116 B]
Get:32 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:33 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:34 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [6840 B]
Get:35 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [9652 B]
Get:36 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [17.6 kB]
Get:37 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [116 B]
Get:38 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:39 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:40 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:41 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:42 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [158 kB]
Get:43 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [41.5 kB]
Get:44 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [6876 B]
Get:45 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [44.4 kB]
Get:46 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [17.0 kB]
Get:47 https://apt.grafana.com stable/main amd64 Packages [250 kB]
Get:48 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:49 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [112 B]
Get:50 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [70.1 kB]
Get:51 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [14.3 kB]
Get:52 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:53 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:54 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [116 B]
Fetched 29.4 MB in 6s (4962 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-14-188:~$ sudo apt-get install grafana-enterprise
```

To install the latest Enterprise release:
sudo apt-get install grafana-enterprise

```
aws Services Search [Alt+S] Mumbai rahul @ 9054-1844-7105
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 musl amd64 1.2.4-2 [416 kB]
Get:2 https://apt.grafana.com stable/main amd64 grafana-enterprise amd64 11.0.0 [120 MB]
Fetched 121 MB in 11s (10.5 MB/s)
Selecting previously unselected package musl:amd64.
(Reading database ... 71839 files and directories currently installed.)
Preparing to unpack .../musl_1.2.4-2_amd64.deb ...
Unpacking musl:amd64 (1.2.4-2) ...
Selecting previously unselected package 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.
ubuntu@ip-172-31-14-188:~$ sudo systemctl start grafana-server
```

- *sudo systemctl start grafana-server*
- *sudo systemctl enable grafana-server.service*


```
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=provisioning.dashboard t=2024-06-18T15:11:38.331125089Z level=info msg="starting to provision dashboards"
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=provisioning.dashboard t=2024-06-18T15:11:38.331155154Z level=info msg="finished to provision dashboards"
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=http.server t=2024-06-18T15:11:38.380358573Z level=info msg="HTTP Server listen" address=[::]:3000 protocol=
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=sqlstore.transactions t=2024-06-18T15:11:38.493822724Z level=info msg="Database locked, sleeping then retryin
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=sqlstore.transactions t=2024-06-18T15:11:38.516065191Z level=info msg="Database locked, sleeping then retryin
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=plugins.update.checker t=2024-06-18T15:11:38.853932226Z level=info msg="Update check succeeded" duration=554
Jun 18 15:11:38 ip-172-31-14-188 grafana[2028]: logger=grafana.update.checker t=2024-06-18T15:11:38.874267515Z level=info msg="Update check succeeded" duration=580
Jun 18 15:11:39 ip-172-31-14-188 grafana[2028]: logger=plugin.angular detectorsprovider.dynamic t=2024-06-18T15:11:39.007963038Z level=info msg="Patterns update fin
Jun 18 15:11:39 ip-172-31-14-188 grafana[2028]: logger=grafana-apiserver t=2024-06-18T15:11:39.383980342Z level=info msg="Adding GroupVersion playlist.grafana.app
Jun 18 15:11:39 ip-172-31-14-188 grafana[2028]: logger=grafana-apiserver t=2024-06-18T15:11:39.384644464Z level=info msg="Adding GroupVersion featuretoggle.grafana

ubuntu@ip-172-31-14-188:~$ 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
Created symlink /etc/systemd/system/multi-user.target.wants/grafana-server.service → /usr/lib/systemd/system/grafana-server.service.
ubuntu@ip-172-31-14-188:~$ sudo systemctl status grafana-server
```

sudo systemctl status grafana-server.service

```
aws Services Search [Alt+S] Mumbai rahul @ 9054-1844

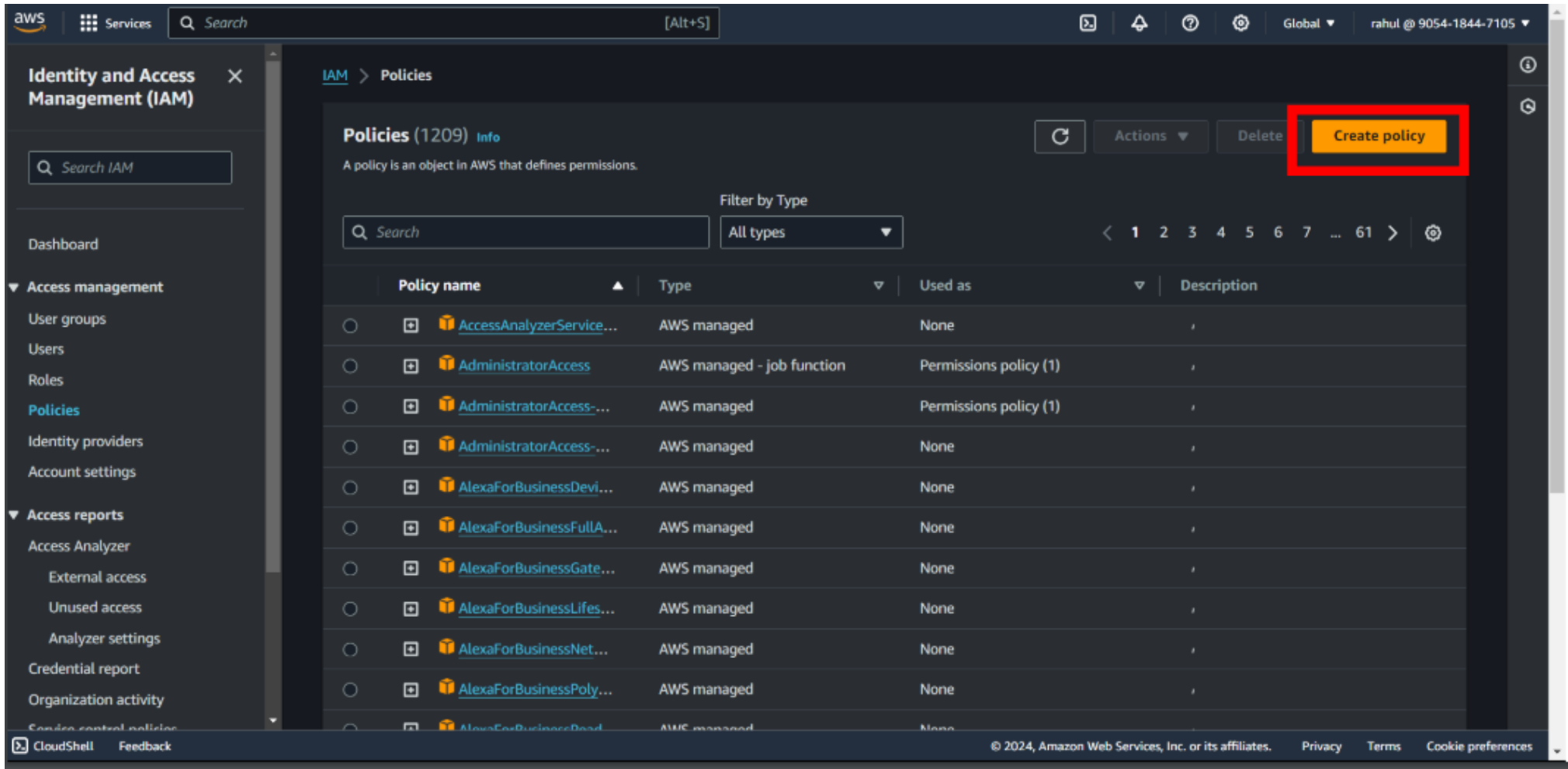
no services need to be restarted.

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.
ubuntu@ip-172-31-14-188:~$ sudo systemctl start grafana-server
ubuntu@ip-172-31-14-188:~$ sudo systemctl status grafana-server
grafana-server.service - Grafana instance
Loaded: loaded (/usr/lib/systemd/system/grafana-server.service; disabled; preset: enabled)
Active: active (running) since Tue 2024-06-18 15:11:29 UTC; 21s ago
Docs: https://grafana.com/docs
Main PID: 2028 (grafana)
Tasks: 16 (limit: 1130)
Memory: 88.9M (peak: 89.3M)
CPU: 3.284s
```

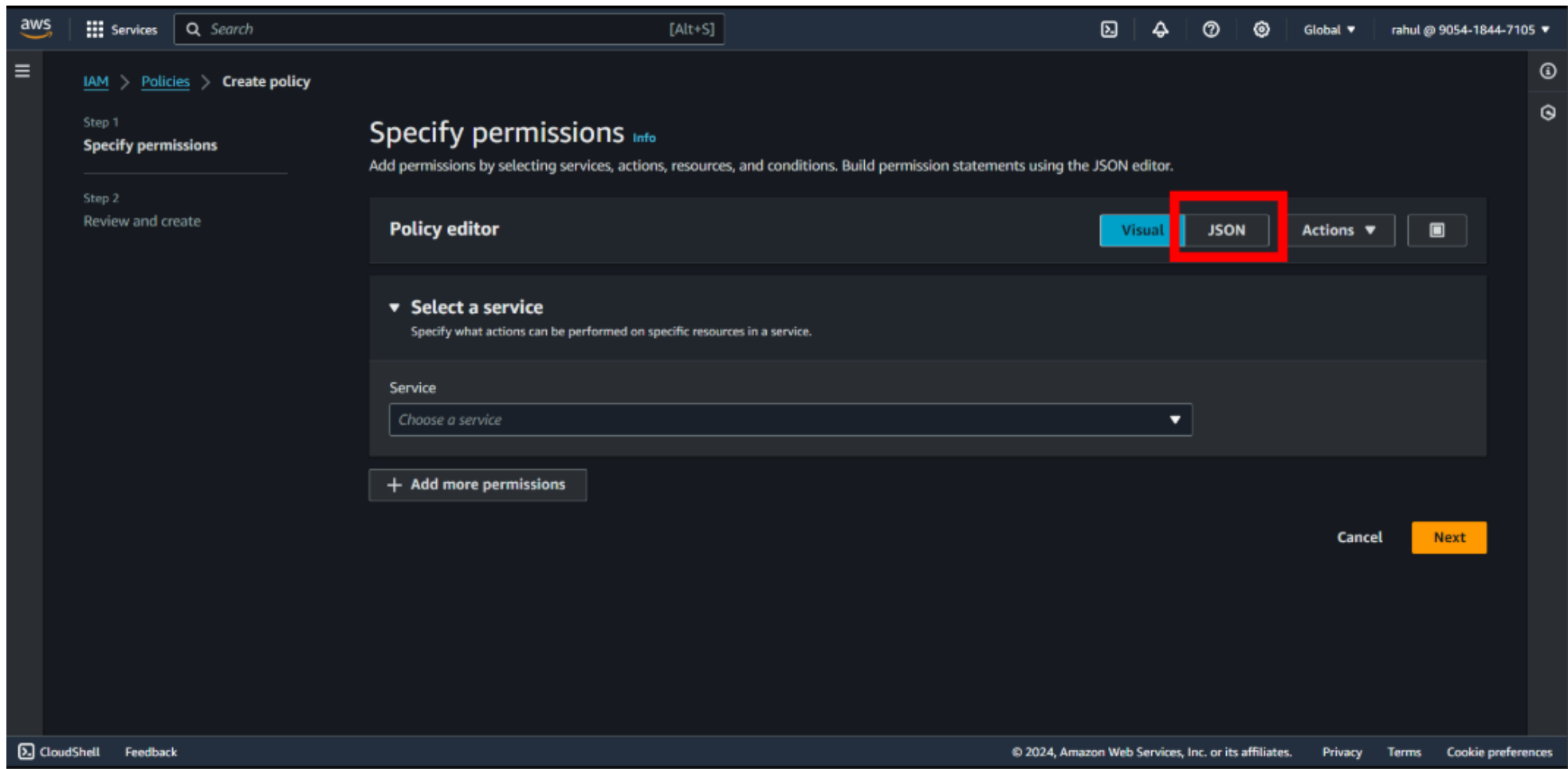
❖ Creating policy:



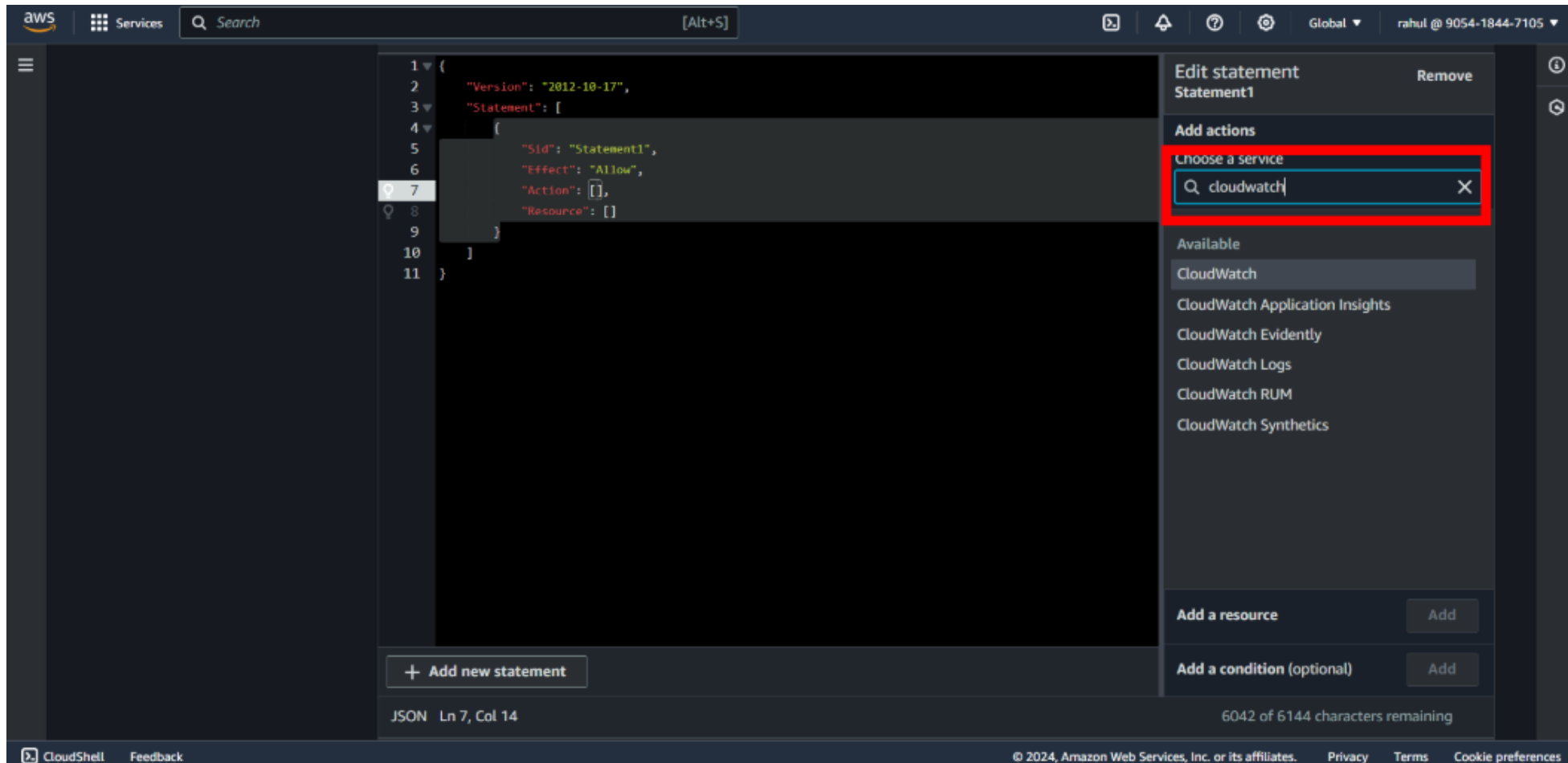
The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area is titled 'Policies (1209)' and includes a search bar, a 'Filter by Type' dropdown set to 'All types', and a table of policies. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. A red rectangular box highlights the 'Create policy' button in the top right corner of the main content area.

	Policy name	Type	Used as	Description
<input type="radio"/>	AccessAnalyzerService...	AWS managed	None	,
<input type="radio"/>	AdministratorAccess	AWS managed - job function	Permissions policy (1)	,
<input type="radio"/>	AdministratorAccess-...	AWS managed	Permissions policy (1)	,
<input type="radio"/>	AdministratorAccess-...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessDevi...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessFullA...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessGate...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessLifes...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessNet...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessPoly...	AWS managed	None	,
<input type="radio"/>	AlexaForBusinessDevi...	AWS managed	None	,

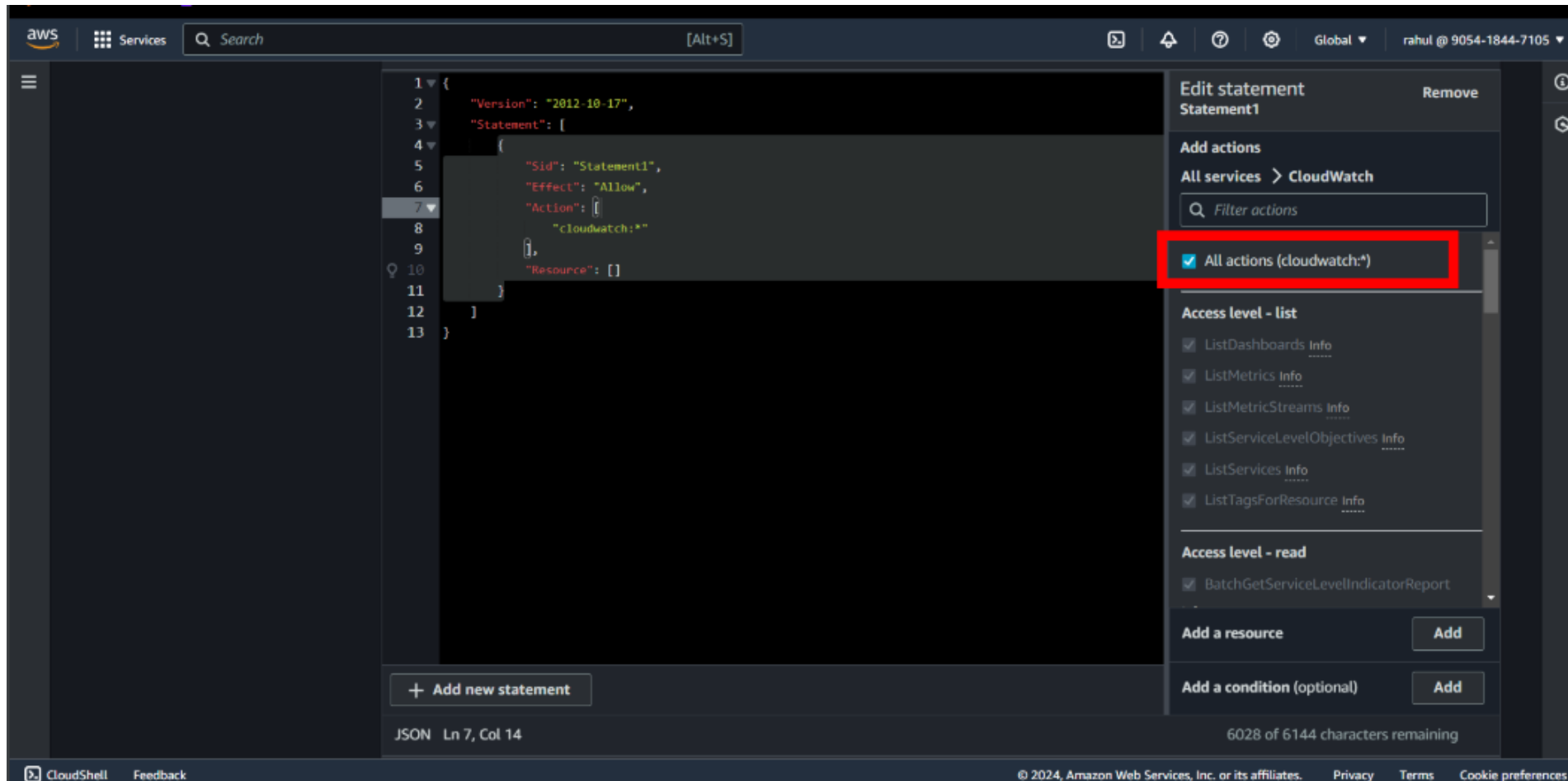
- Then search IAM role and go to policies and click on **Create policies**.



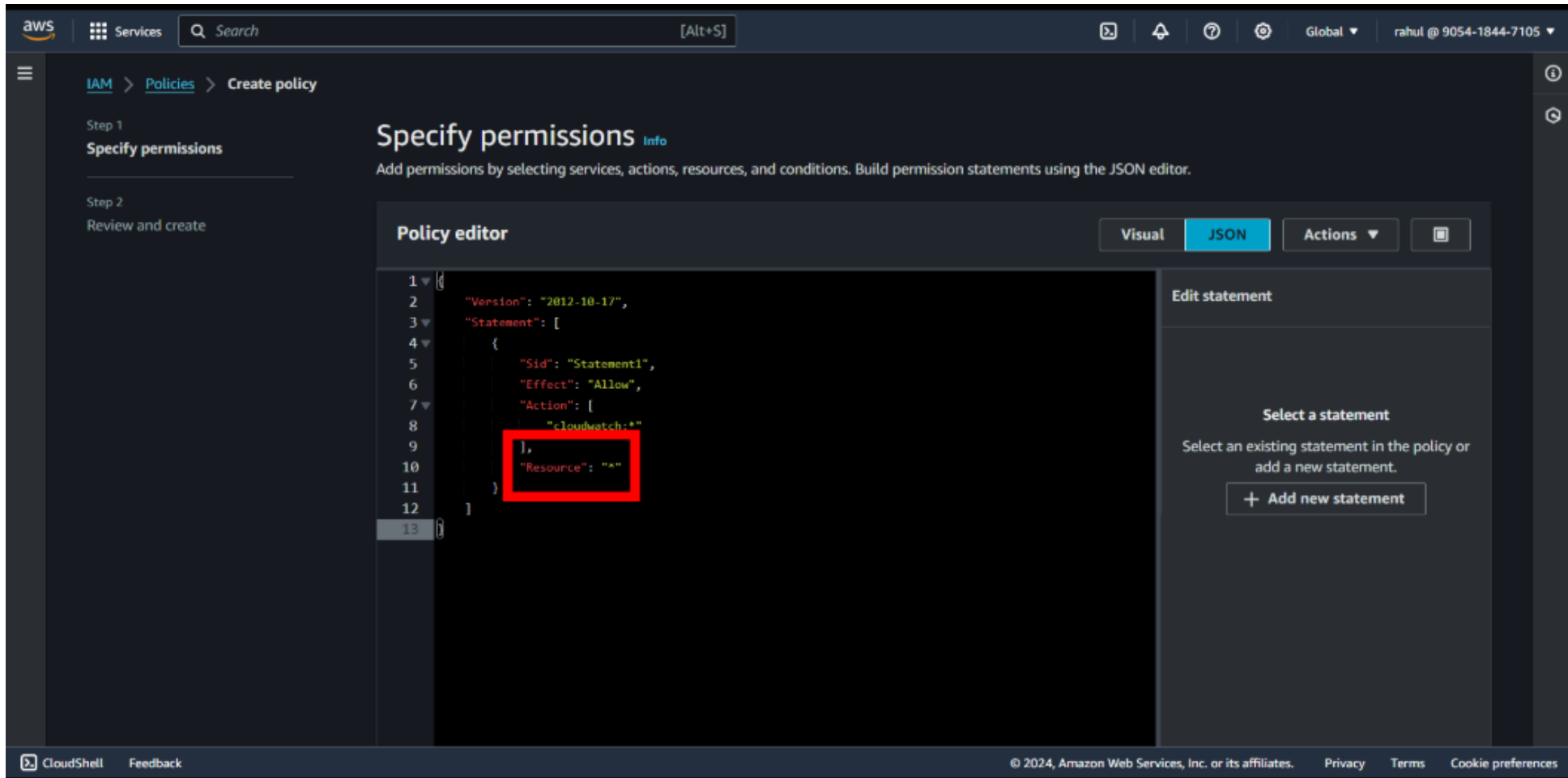
- Then go to **JSON** type.



- Click on add action and search for **“Cloudwatch”**.



- After selecting cloudwatch select **“All actions”**.



- Then put “Resource “ : ”*”

aws Services Search [Alt+S]

Maximum 1,000 characters. Use alphanumeric and '+=,@-_' characters.

Permissions defined in this policy [Info](#) [Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

Allow (1 of 417 services) ☐ Show remaining 416 services

Service	Access level	Resource	Request condition
CloudWatch	Full access	All resources	None

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

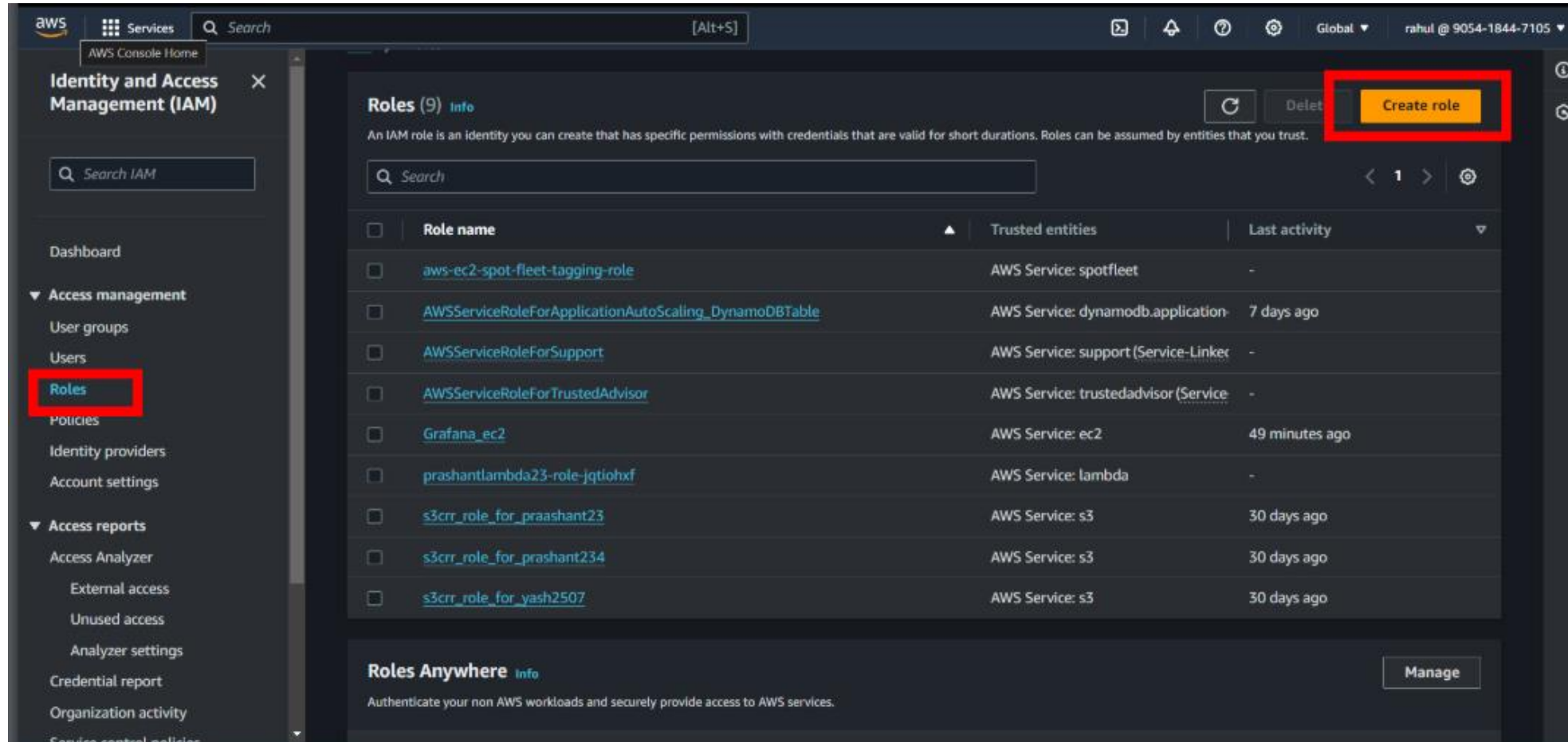
You can add up to 50 more tags.

Cancel Previous **Create policy**

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Scroll down and click on **Create policy**.

❖ Creating role :

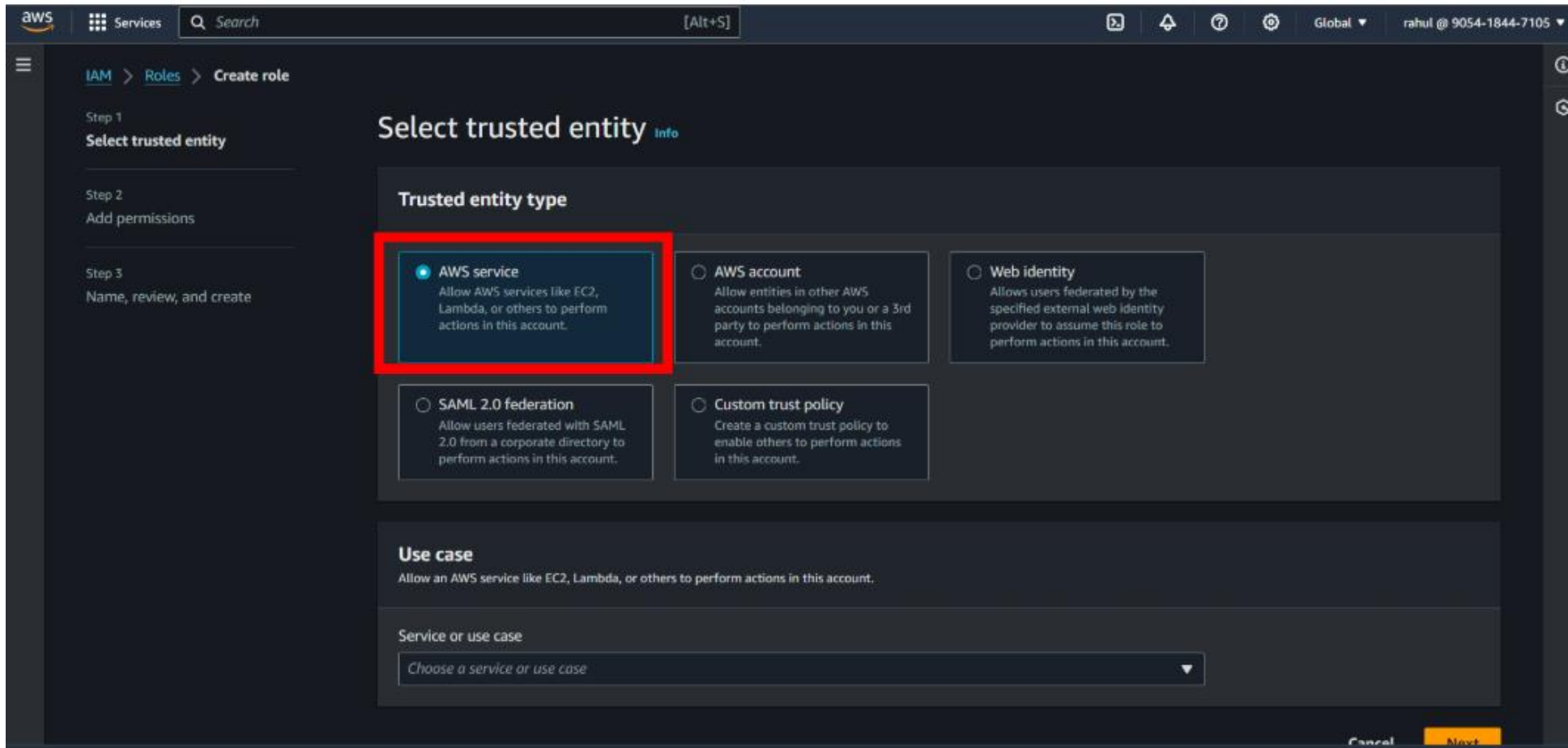


The screenshot shows the AWS IAM console interface. In the left-hand navigation pane, the 'Roles' link under 'Access management' is highlighted with a red rectangle. In the top right corner of the main content area, the 'Create role' button is also highlighted with a red rectangle. The main content area displays the 'Roles (9)' page, which includes a search bar and a table of roles.

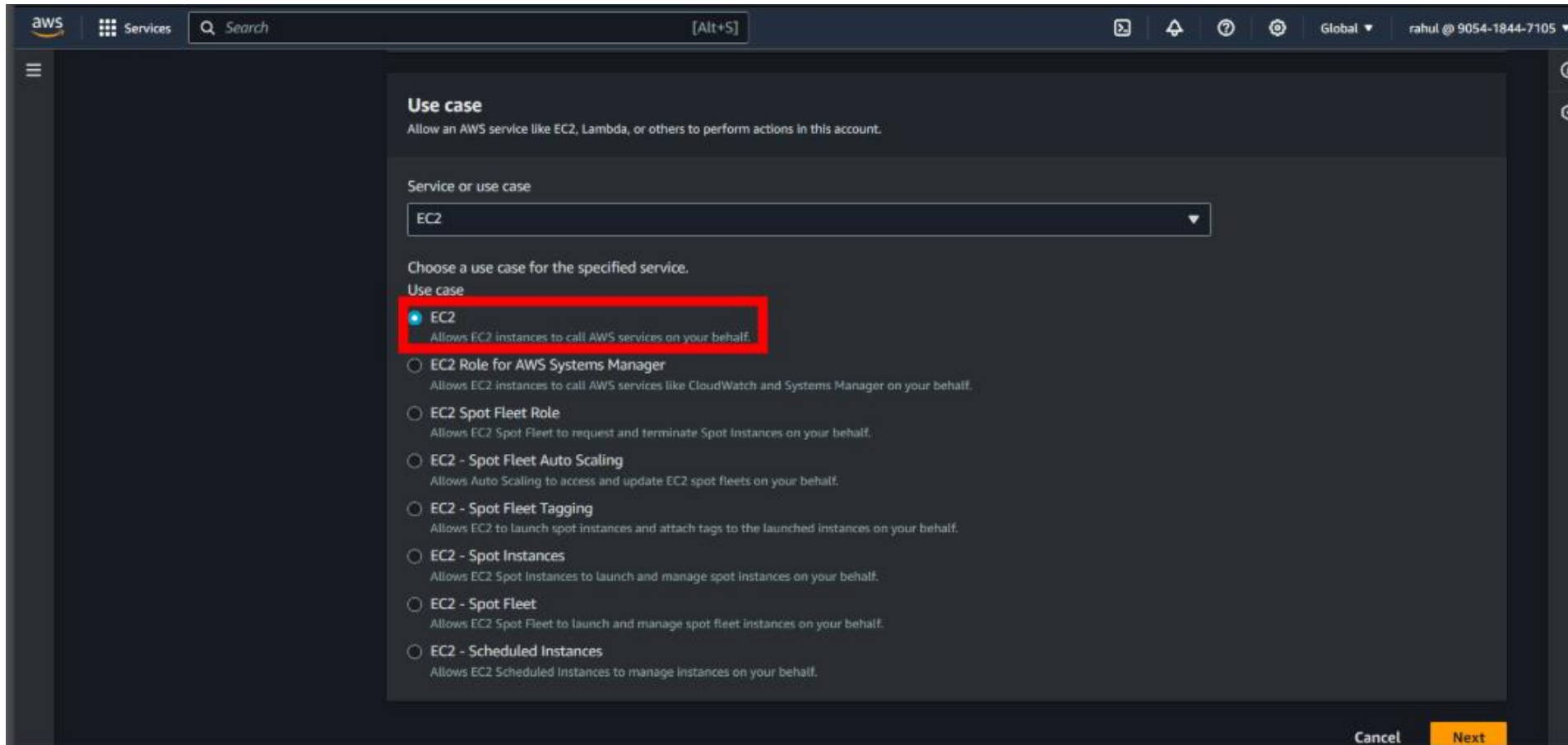
<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	aws-ec2-spot-fleet-tagging-role	AWS Service: spotfleet	-
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-	7 days ago
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linker	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
<input type="checkbox"/>	Grafana_ec2	AWS Service: ec2	49 minutes ago
<input type="checkbox"/>	prashantlambda23-role-jqtiohxf	AWS Service: lambda	-
<input type="checkbox"/>	s3crr_role_for_praashant23	AWS Service: s3	30 days ago
<input type="checkbox"/>	s3crr_role_for_prashant234	AWS Service: s3	30 days ago
<input type="checkbox"/>	s3crr_role_for_yash2507	AWS Service: s3	30 days ago

At the bottom of the console, there is a section titled 'Roles Anywhere' with a 'Manage' button.

- Then go to roles and click on **Create roles**.



- Then select entity type is **AWS services** .



- Now , select use case as **EC2** .

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selectedUseCase=EC2

aws Search [Alt+S] Global farhan @ 4401-2484-1385

IAM > Roles > Create role

step 3
Name, review, and create

Filter by Type

grafana All types 8 matches

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonGrafanaAthenaAccess	AWS managed	This policy grants access to Amazon At...
<input type="checkbox"/>	AmazonGrafanaCloudWatchAcc...	AWS managed	This policy grants access to Amazon Cl...
<input type="checkbox"/>	AmazonGrafanaRedshiftAccess	AWS managed	This policy grants scoped access to Am...
<input type="checkbox"/>	AWSGrafanaAccountAdministrator	AWS managed	Provides access within Amazon Grafan...
<input type="checkbox"/>	AWSGrafanaConsoleReadOnlyA...	AWS managed	Access to read only operations in Ama...
<input type="checkbox"/>	AWSGrafanaWorkspacePermissi...	AWS managed	Provides only the ability to update use...
<input type="checkbox"/>	AWSGrafanaWorkspacePermissi...	AWS managed	Provides ability to update IAM Identity...
<input type="checkbox"/>	grafana	Customer managed	-

► Set permissions boundary - optional

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search 30°C Mostly clear 12:30 AM 6/26/2025

- Select your policy here which you have created previously , then click on **Next**.

The screenshot shows the AWS IAM console interface for creating a new role. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and a user profile 'rahul @ 9054-1844-7105'. The left sidebar shows the breadcrumb 'IAM > Roles > Create role' and a list of steps: 'Step 1: Select trusted entity', 'Step 2: Add permissions', and 'Step 3: Name, review, and create'. The main content area is titled 'Name, review, and create' and contains a 'Role details' section. This section has two input fields: 'Role name' and 'Description'. The 'Role name' field is highlighted with a red rectangular box. Below the 'Role name' field is a 'Description' field with the text 'Allows EC2 instances to call AWS services on your behalf.' and a character limit note: 'Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+ = , @ - / \ [] ! # \$ % ^ & * 0 ; : " < > ' '. At the bottom of the page, there is a 'Step 1: Select trusted entities' label and an 'Edit' button.

aws Services Search [Alt+S] Global rahul @ 9054-1844-7105

IAM > Roles > Create role

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.

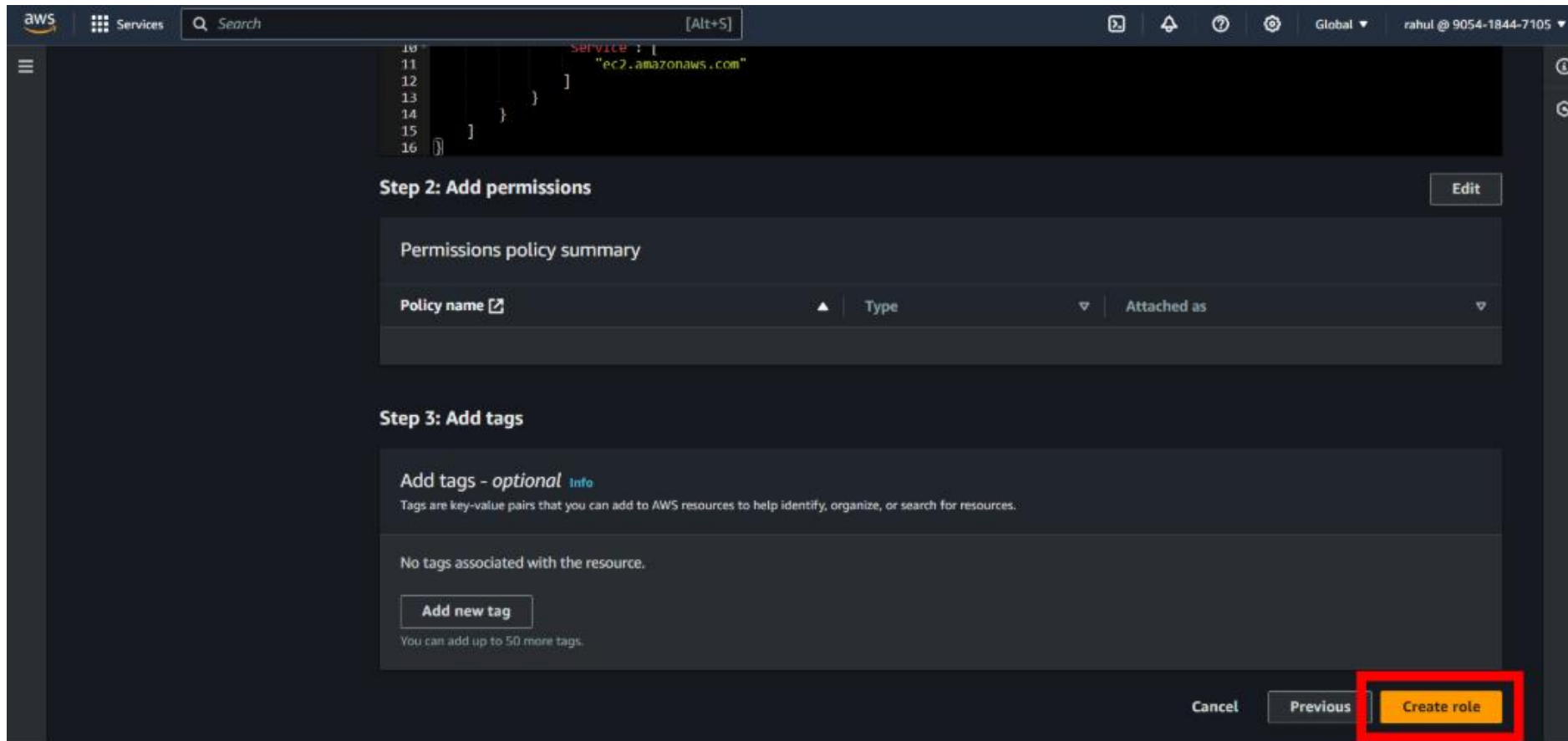
Description
Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

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

Step 1: Select trusted entities Edit

- Then give a name of your choice to the role .



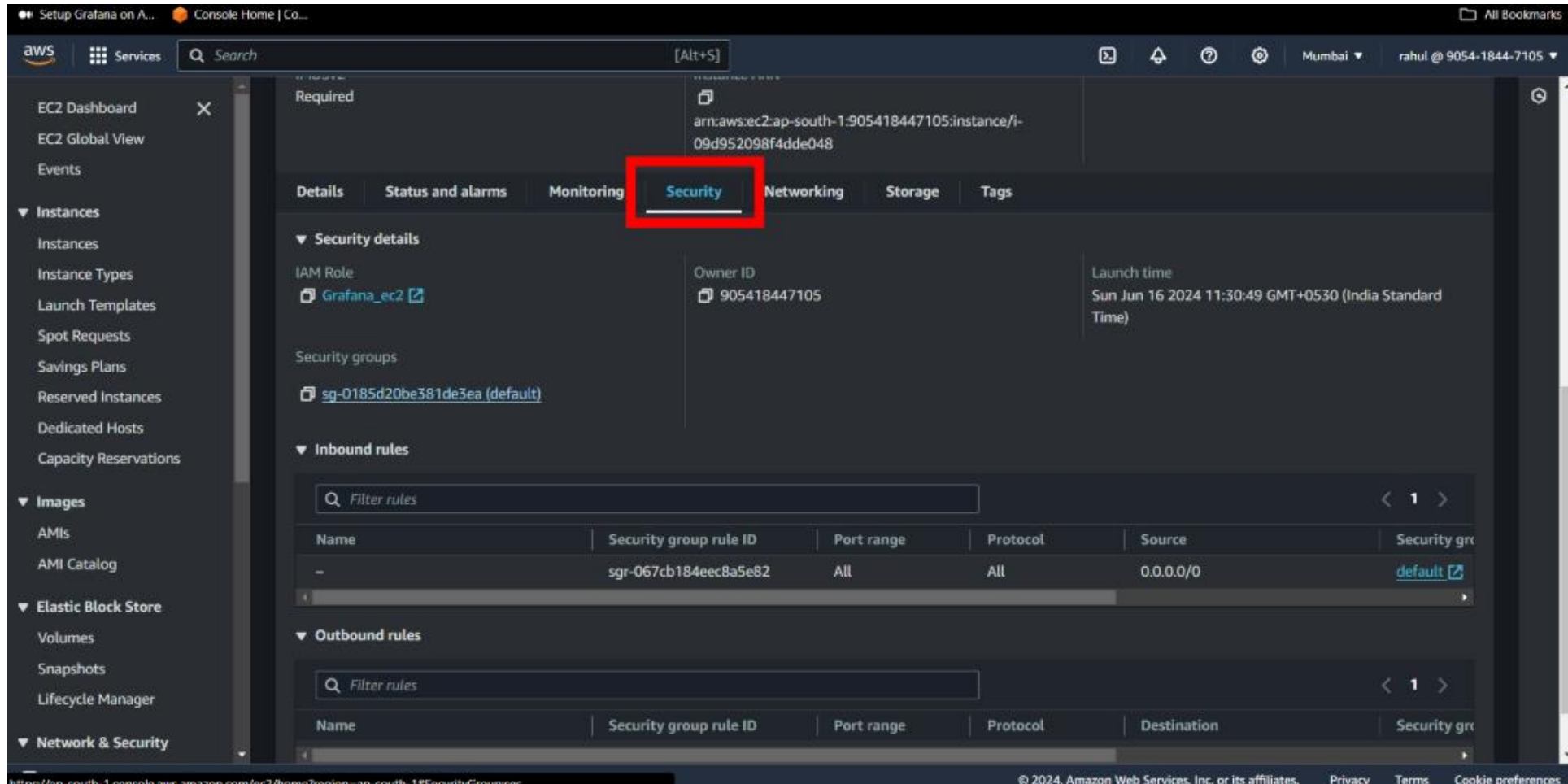
- Then scroll down and click on the **Create role** .

The screenshot displays the AWS Management Console for the 'ap-south-1' region. The main content area shows the 'Instances (1)' page with a table of EC2 instances. The instance 'grafana' is listed with ID 'i-0f4451f8477b79674', state 'Running', type 't2.micro', and is located in 'ap-south-1b'. The left sidebar contains navigation links for EC2 services. The bottom of the image shows a Windows taskbar with a search bar, application icons, and system tray information including the date and time.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
grafana	i-0f4451f8477b79674	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-65-2

- After creating your role and policy go to instance and open your instance , which you have already created.

❖ Modifying security rules:



- Scroll down and go to **Security** option.

The screenshot displays the AWS Management Console interface for a security group. The breadcrumb navigation at the top indicates the path: **EC2** > **Security Groups** > **sg-0185d20be381de3ea - default**. The main heading is **sg-0185d20be381de3ea - default**, with an **Actions** dropdown menu to its right.

The **Details** section provides key information about the security group:

Property	Value
Security group name	default
Security group ID	sg-0185d20be381de3ea
Description	default VPC security group
VPC ID	vpc-0fd125980362775a9
Owner	905418447105
Inbound rules count	1 Permission entry
Outbound rules count	1 Permission entry

Below the details, there are tabs for **Inbound rules**, **Outbound rules**, and **Tags**. The **Inbound rules** tab is active, showing **Inbound rules (1)**. A search bar is present above the rule list. The rule list contains one entry:

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-067cb184eec8a5e82	IPv4	All traffic	All	All

At the top right of the rule list, there are buttons for **Manage tags** and **Edit inbound rules**. The **Edit inbound rules** button is highlighted with a red rectangle.

- Then click on **Edit inbound rule** .

aws Services Search [Alt+S] Mumbai rahul @ 9054-1844-7105


EC2 > Security Groups > sg-0185d20be381de3ea - default > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
sgr-067cb184eec8a5e82	All traffic ▼	All	All	Custom ▼	<input type="text" value="Q"/>	<input type="text" value="0.0.0.0/0 X"/>
<input type="button" value="Delete"/>						

 Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

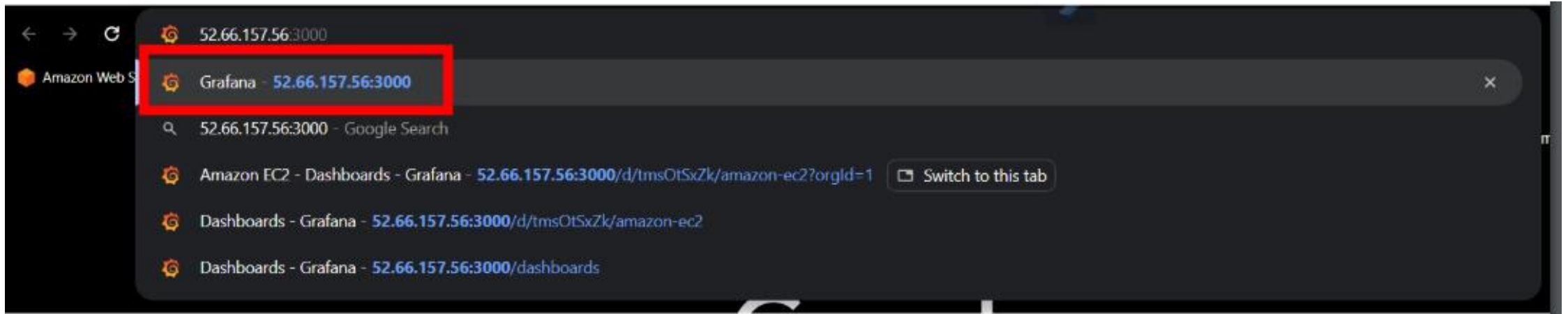
- Then modify your rule **select type = All traffic** and **source =0.0.0.0/0**

The screenshot displays the AWS Management Console interface for an EC2 instance. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, and Network & Security. The main content area shows the 'Instance summary for i-09d952098f4dde048 (rahul ec2)'. The instance is in a 'Running' state. A red box highlights the 'Public IPv4 address' field, which displays '52.66.157.56' with a link to 'open address'. Other fields include 'Private IPv4 addresses' (172.31.43.167), 'Public IPv4 DNS' (ec2-52-66-157-56.ap-south-1.compute.amazonaws.com), 'Elastic IP addresses' (none), 'AWS Compute Optimizer finding' (Opt-in to AWS Compute Optimizer for recommendations), 'Auto Scaling Group name' (none), 'Instance ID' (i-09d952098f4dde048), 'IPv6 address' (none), 'Hostname type' (IP name: ip-172-31-43-167.ap-south-1.compute.internal), 'Answer private resource DNS name IPv4 (A)' (52.66.157.56 [Public IP]), 'IAM Role' (Grafana_ec2), 'IMDSv2' (Required), 'Instance state' (Running), 'Private IP DNS name (IPv4 only)' (ip-172-31-43-167.ap-south-1.compute.internal), 'Instance type' (t2.micro), 'VPC ID' (vpc-0fd125980362775a9), 'Subnet ID' (subnet-049d80f66c0e59d7e), and 'Instance ARN' (arn:aws:ec2:ap-south-1:905418447105:instance/i-09d952098f4dde048).

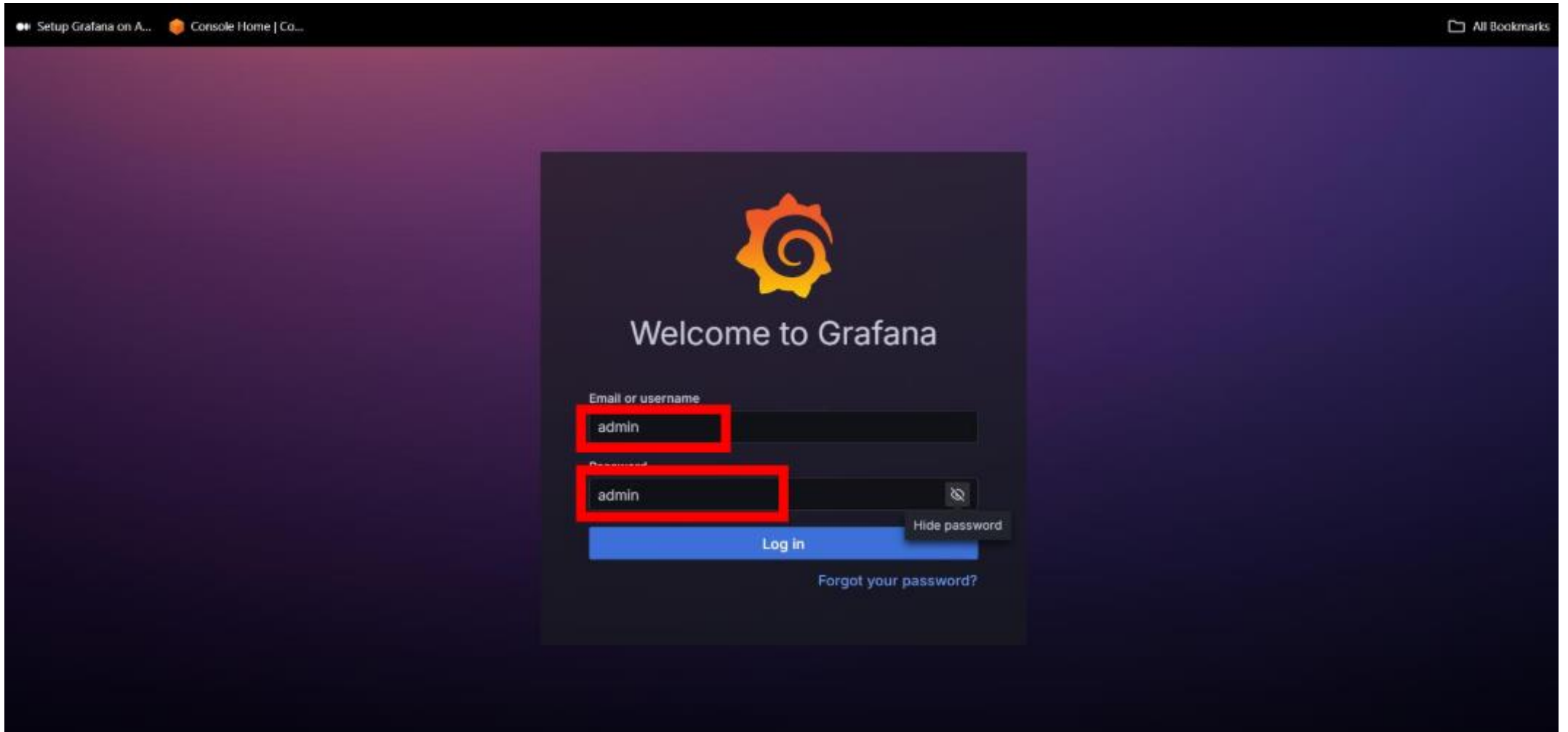
Field	Value
Instance ID	i-09d952098f4dde048 (rahul ec2)
Public IPv4 address	52.66.157.56 open address
Private IPv4 addresses	172.31.43.167
Public IPv4 DNS	ec2-52-66-157-56.ap-south-1.compute.amazonaws.com open address
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto Scaling Group name	-
Instance state	Running
Private IP DNS name (IPv4 only)	ip-172-31-43-167.ap-south-1.compute.internal
Instance type	t2.micro
VPC ID	vpc-0fd125980362775a9
Subnet ID	subnet-049d80f66c0e59d7e
Instance ARN	arn:aws:ec2:ap-south-1:905418447105:instance/i-09d952098f4dde048
IPv6 address	-
Hostname type	IP name: ip-172-31-43-167.ap-south-1.compute.internal
Answer private resource DNS name IPv4 (A)	52.66.157.56 [Public IP]
Auto-assigned IP address	52.66.157.56 [Public IP]
IAM Role	Grafana_ec2
IMDSv2	Required

- Then copy your **public IPv4 address** of your instance .

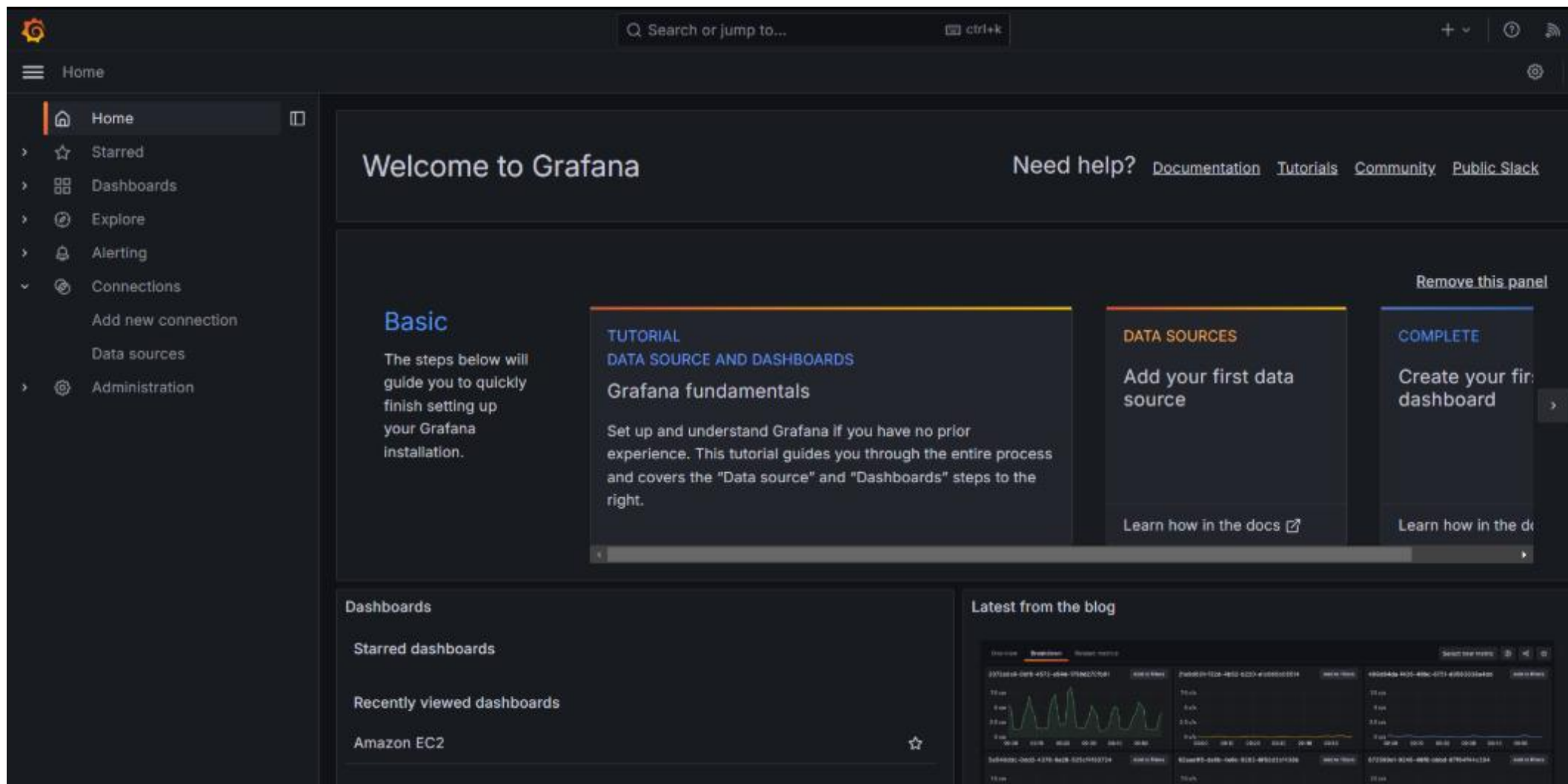
❖ Starting GRAFANA:



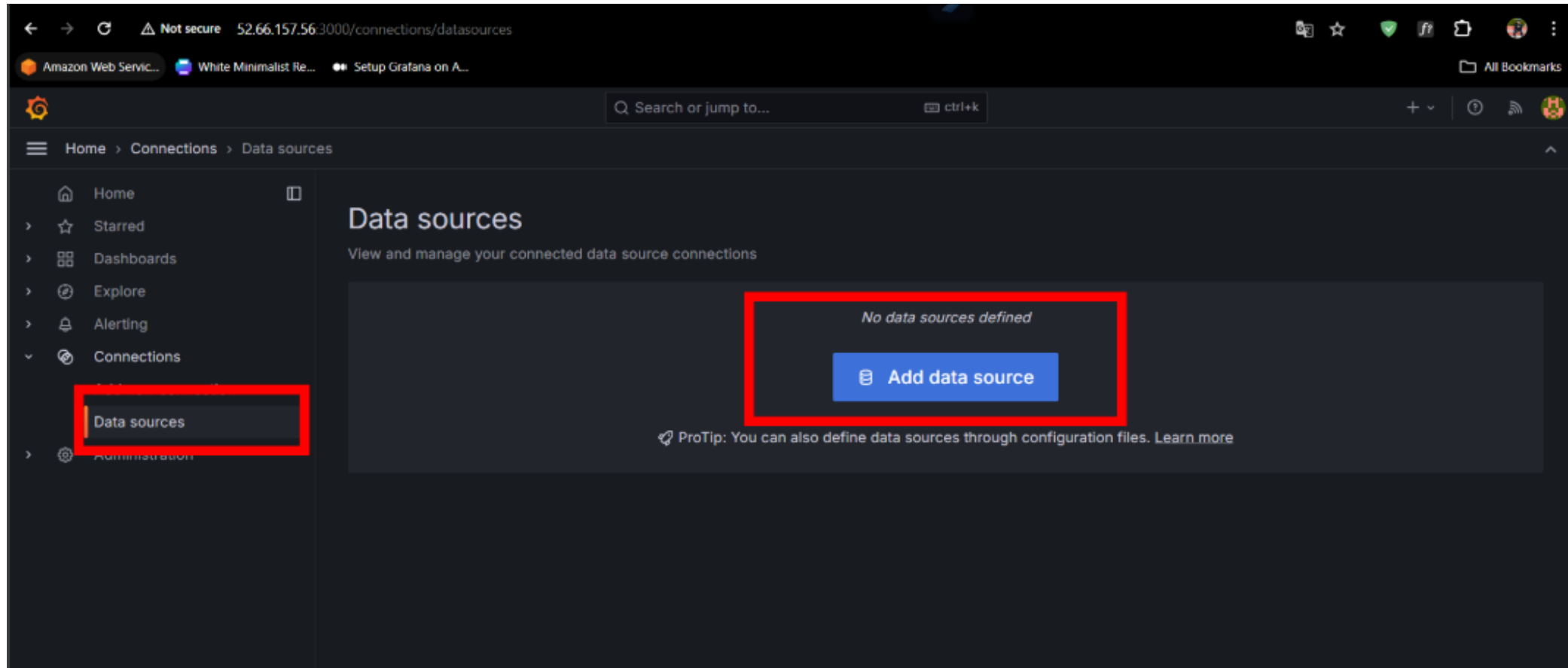
- Then paste your copied ip address and type “:3000” after ip address and search it .



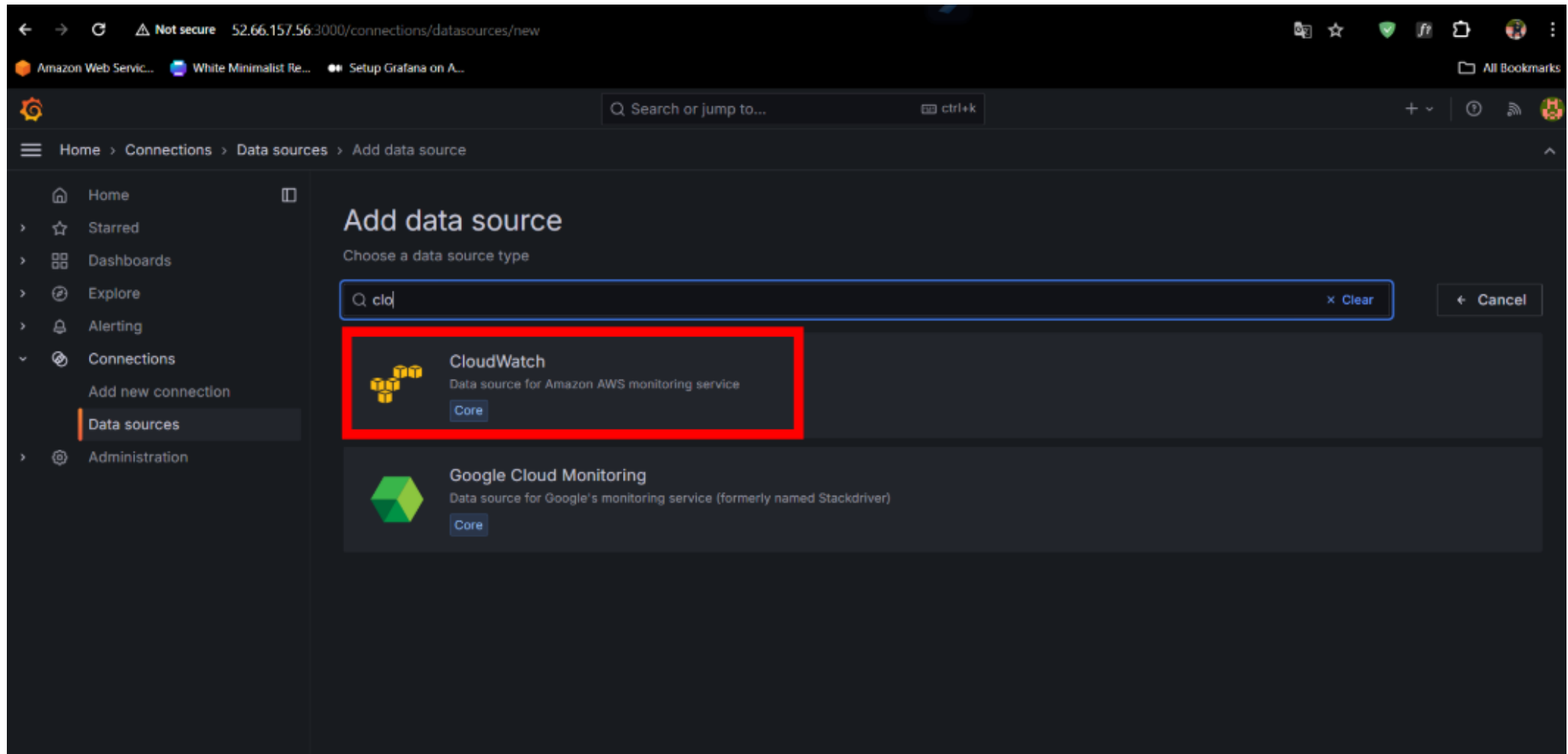
- Then login in Grafana by the help of credentials shown in above snapshot.



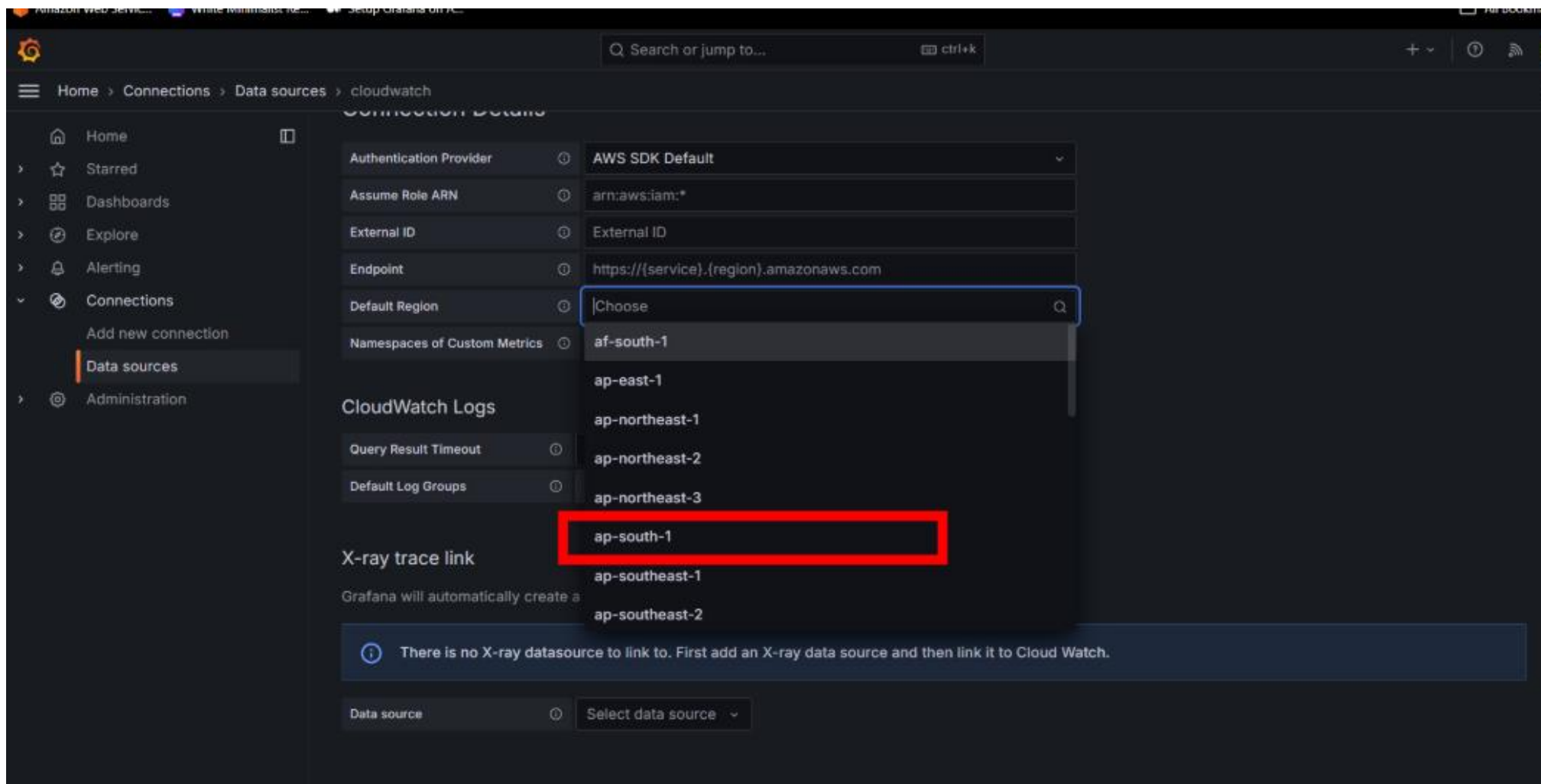
❖ Adding data source to grafana :



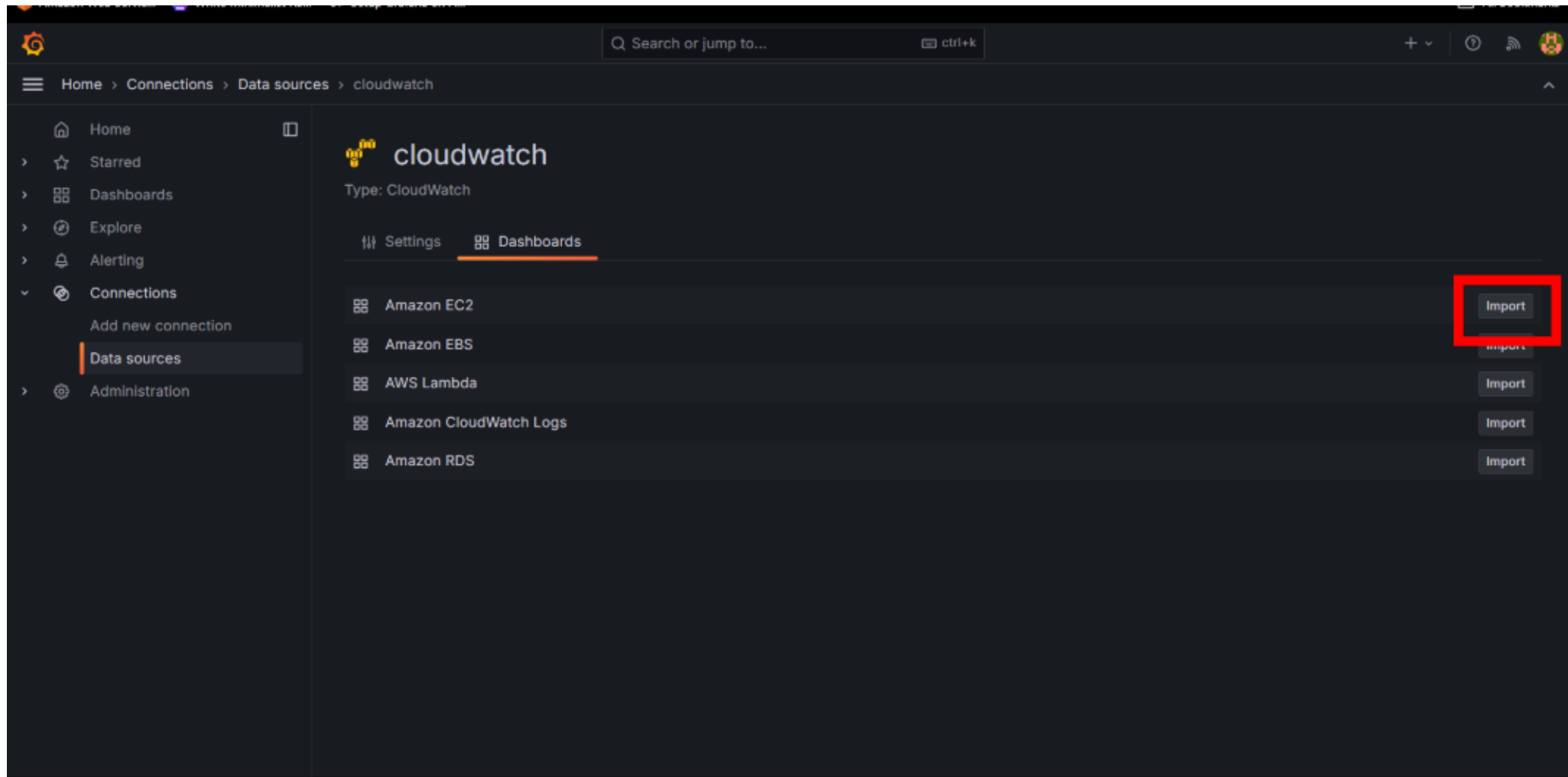
- Then go to **Dashboard** and click on **Add data source** .



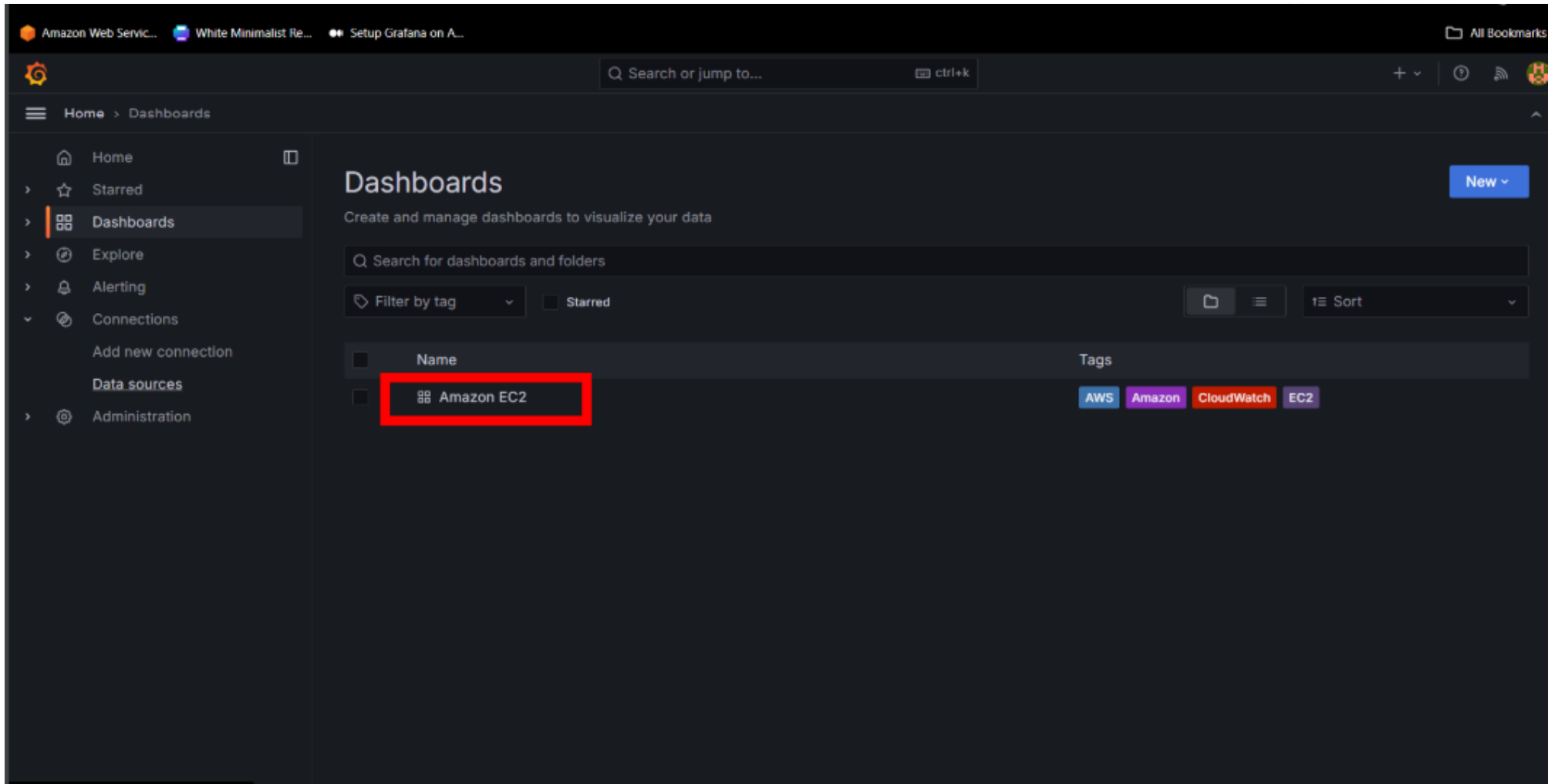
- Now , select “**Cloudwatch**” as an data source .



- Then after selecting cloudwatch select your region .



- Then inside your cloudwatch go to dashboard and **Import EC2**.



- Then go to dashboard and open your **Amazon EC2**.

❖ Graph of CPU utilization in GRAFANA :

