

CLOUD WATCH - AWS

CLOUD WATCH:

- It is used for various purposes like MONITORING, ALARMS, DASHBOARDS, LOGS AND SCALING
- It is used to monitor various AWS services.
- It allows us to record metrics for aws services like EC2, EBS, ELB AND Amazon S3.
- We can setup alarms for our EC2 Instances

PROJECT-1: CREATE ALARM FOR AN EC2-INSTANCE

HOW IT WORKS:

- Once we launch an instance if the CPU utilisation of instance is above 80% then alarm will be triggered
- Once alarm is triggered you will get notified by SNS service

HOW TO SETUP:

STEP-1: LAUNCH AN EC2-INSTANCE

Instances (1/1) [Info](#)

Find instance by attribute or tag (case-sensitive)

Instance state = running X Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Cloud-watch	i-01b2538643a316ac0	Running	t2.micro	2/2 checks passed	No alarms

Instance: i-01b2538643a316ac0 (Cloud-watch)

Details | Security | Networking | Storage | Status checks | **Monitoring** | Tags

Manage detailed monitoring

1h 3h 12h 1d 3d 1w Custom Add to dashboard

CPU utilization (%)

No unit No data available.
Try adjusting the dashboard time range.

0.5

0

17:15 18:15

Status check failed (any) (c...

No unit No data available.
Try adjusting the dashboard time range.

0.5

0

17:15 18:15

Status check failed (instanc...

No unit No data available.
Try adjusting the dashboard time range.

0.5

0

17:15 18:15

Status check failed (system...

No unit No data available.
Try adjusting the dashboard time range.

0.5

0

17:15 18:15

Network in (bytes)

No unit No data available.
Try adjusting the dashboard time range.

0.5

Network out (bytes)

No unit No data available.
Try adjusting the dashboard time range.

0.5

Network packets in (count)

No unit No data available.
Try adjusting the dashboard time range.

0.5

Network packets out (count)

No unit No data available.
Try adjusting the dashboard time range.

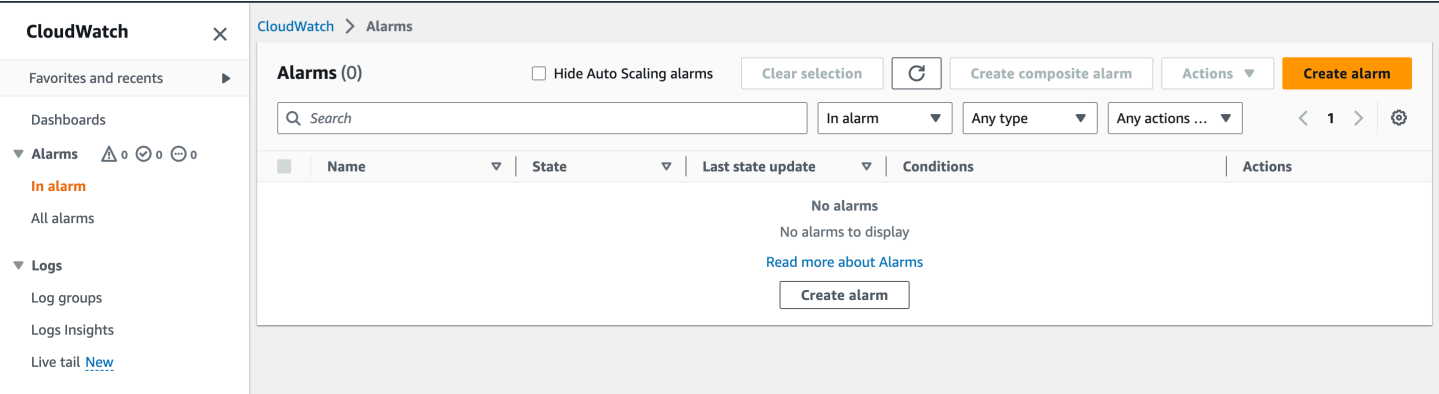
0.5

After launching the instance, check in monitoring tab no data is available. because we just created this instance

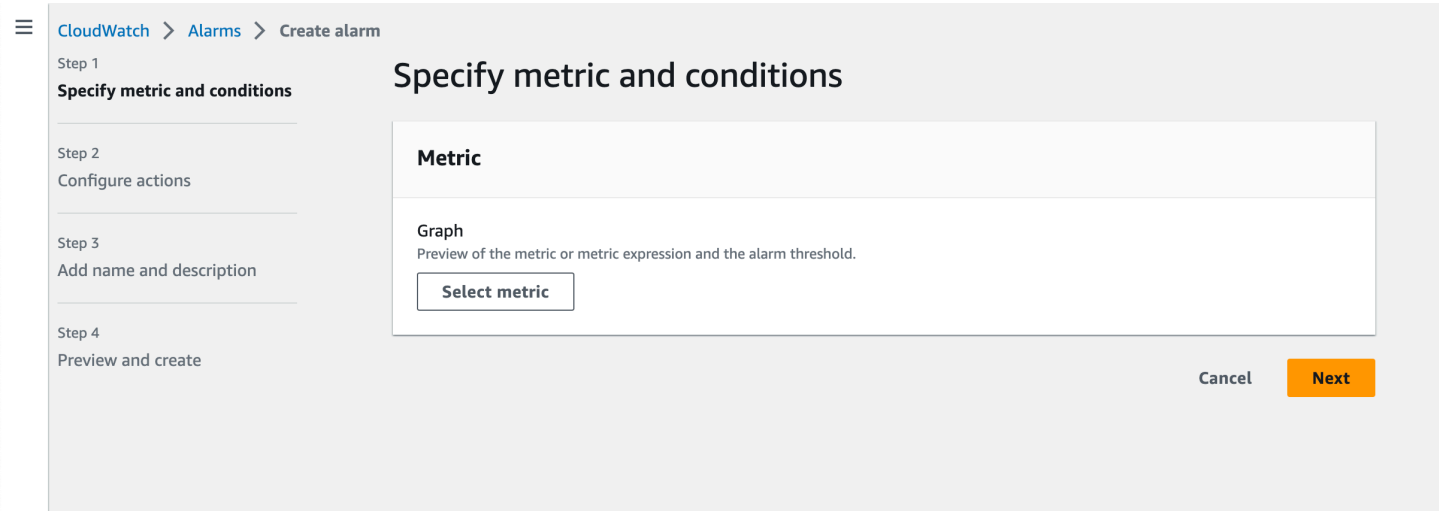
HERE OUR ULTIMATE AIM IS TO MONITOR THE INSTANCE, WHEN CPU UTILISATION IS MORE THAN 50% THEN WE HAVE TO GET A MAIL. SO WE CAN PERFORM THE ACTION AS PER THE REQUIREMENT.

STEP-2: OPEN CLOUD WATCH AND SET AN ALARM

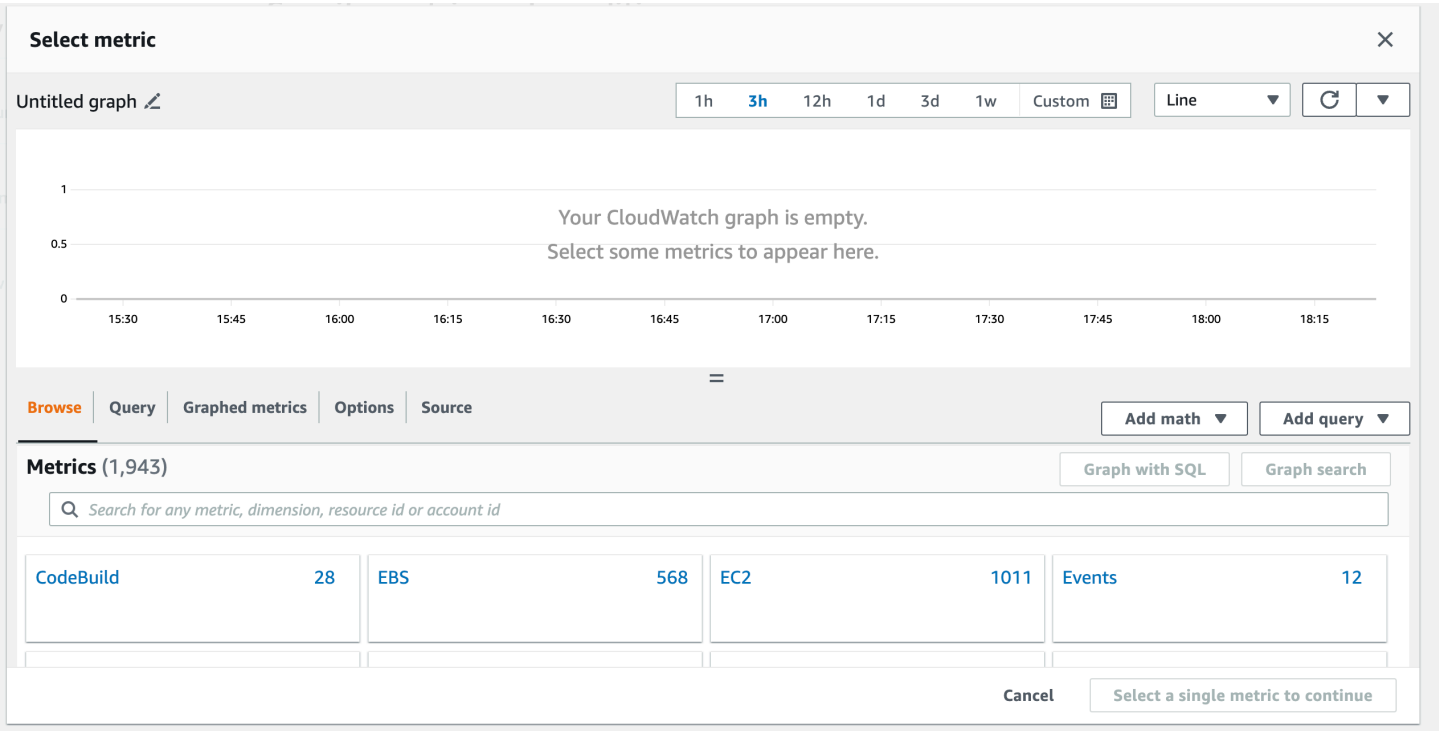
Open cloud watch service in console and select alarm



Click on create alarm



click on select metrics



select EC2

Select metric

×

Untitled graph ↗

1h3h12h1d3d1wCustom

Line

↺↻

1

0.5

0

15:3015:4516:0016:1516:3016:4517:0017:1517:3017:4518:0018:15

Your CloudWatch graph is empty.
Select some metrics to appear here.

BrowseQueryGraphed metricsOptionsSource

Add mathAdd query

Metrics (1,011)

Graph with SQLGraph search

All > EC2

Search for any metric, dimension, resource id or account id

By Auto Scaling Group34

By Image (AMI) Id7

Per-Instance Metrics956

Aggregated by Instance Type7

Across All Instances7

Cancel

Select a single metric to continue

select Pre-Instance Metrics and then you will get a lot of instances like this

Select metric

×

=

BrowseQueryGraphed metricsOptionsSource

Add mathAdd query

Metrics (956)

Graph with SQLGraph search

All > EC2 > Per-Instance Metrics

Search for any metric, dimension, resource id or account id

< 1 2 3 4 5 > ⚙

☐ InstanceId 100/500 ▲ Metric name ▼

☐ i-000bd589a050a1280 MetadataNoToken

☐ i-000bd589a050a1280 StatusCheckFailed_System

☐ i-000bd589a050a1280 StatusCheckFailed_Instance

☐ i-000bd589a050a1280 StatusCheckFailed

☐ i-000bd589a050a1280 NetworkPacketsIn

☐ i-000bd589a050a1280 NetworkPacketsOut

☐ i-000bd589a050a1280 CPUUtilization

Cancel

Select a single metric to continue

Here we have to select a single metrics for our server,

Search our instance with instance-id

Select metric

Browse

Query

Graphed metrics (1)

Options

Source

Add math

Add query

Metrics (17)

Graph with SQL

Graph search

All > EC2 > Per-Instance Metrics

Q

Search for any metric, dimension, resource id or account id

i-01b2538643a316ac0

	Instanceld	Metric name
<input type="checkbox"/>	i-01b2538643a316ac0	NetworkPacketsIn
<input type="checkbox"/>	i-01b2538643a316ac0	NetworkPacketsOut
<input checked="" type="checkbox"/>	i-01b2538643a316ac0	CPUUtilization
<input type="checkbox"/>	i-01b2538643a316ac0	NetworkIn
<input type="checkbox"/>	i-01b2538643a316ac0	NetworkOut
<input type="checkbox"/>	i-01b2538643a316ac0	DiskReadBytes

Cancel

Select metric

select our instance id with the CPUUtilization and click on select metrics

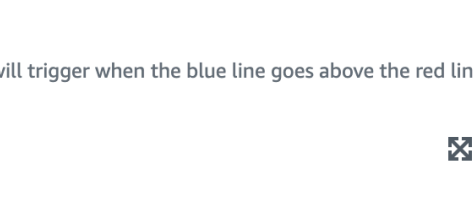
Specify metric and conditions

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.



Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-01b2538643a316ac0

Instance name
Cloud-watch

Statistic
Average

Period
1 minute

In this section we have to select the period, by default it will be 5 minutes but i have changes to 1 minute. And continue the second section which is conditions.

Conditions

Threshold type

☒ Static
Use a value as a threshold

☐ Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

☒ Greater
> threshold

☐ Greater/Equal
≥ threshold

☐ Lower/Equal
≤ threshold

☐ Lower
< threshold

than...

Define the threshold value.

10000

Must be a number

► Additional configuration

Cancel

Next

here we have to specify the CPU Utilization, i preferred to take 50%

Conditions

Threshold type

☒ Static

Use a value as a threshold

☐ Anomaly detection

Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

☒ Greater

> threshold

☐ Greater/Equal

>= threshold

☐ Lower/Equal

<= threshold

☐ Lower

< threshold

than...

Define the threshold value.

50

Must be a number

► Additional configuration

Cancel

Next

click on Next

Configure actions

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

☒ In alarm

The metric or expression is outside of the defined threshold.

☐ OK

The metric or expression is within the defined threshold.

☐ Insufficient data

The alarm has just started or not enough data is available.

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ Select an existing SNS topic

☐ Create new topic

☐ Use topic ARN to notify other accounts

Send a notification to...

🔍 Select an email list

Only email lists for this account are available.

Add notification

In this step we have to integrate SNS to get notified through our GMAIL. If the SNS topic is already created then you can select but in my case i haven't created so i am creating here.

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ **In alarm**
The metric or expression is outside of the defined threshold.

☐ **OK**
The metric or expression is within the defined threshold.

☐ **Insufficient data**
The alarm has just started or not enough data is available.

Remove

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN to notify other accounts

Create a new topic...
The topic name must be unique.

cloud-watch-status

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

awsanddevops18@gmail.com

user1@example.com, user2@example.com

Create topic

Add notification

i have entered the topic name and my email id and click on create topic

Configure actions

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

☒ **In alarm**

The metric or expression is outside of the defined threshold.

☐ **OK**

The metric or expression is within the defined threshold.

☐ **Insufficient data**

The alarm has just started or not enough data is available.

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ **Select an existing SNS topic**

☐ Create new topic

☐ Use topic ARN to notify other accounts

Send a notification to...

cloud-watch-status



Only email lists for this account are available.

Email (endpoints)

awsanddevops18@gmail.com - [View in SNS Console](#)

Add notification

This will send a notification to our mail, we have to confirm the subscription on our mail.

1 of 564

AWS Notification - Subscription Confirmation

Inbox x

AWS Notifications <no-reply@sns.amazonaws.com>
to me

Tue, 13 Jun, 23:19 (46 minutes ago)

☆ ↶ ⋮

You have chosen to subscribe to the topic:
arn:aws:sns:ap-south-1:184744381800:Default_CloudWatch_Alarms_Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

↶ Reply

↷ Forward

click on confirm subscription and you will get like this



Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

`arn:aws:sns:ap-south-1:184744381800:Default_CloudWatch_Alarms_Topic:6c27ee2a-da0d-4e80-925a-7be3f435bbc4`

If it was not your intention to subscribe, [click here to unsubscribe](#).

After that go back to cloud watch,

Auto Scaling action

Add Auto Scaling action

EC2 action

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

☒ In alarm

The metric or expression is outside of the defined threshold.

☐ OK

The metric or expression is within the defined threshold.

☐ Insufficient data

The alarm has just started or not enough data is available.

Take the following action...

Define what will happen to the EC2 instance with the Instance ID i-01b2538643a316ac0 when this alarm is triggered.

☐ Recover this instance

You can only recover certain EC2 instance types. [See documentation](#)

☐ Stop this instance

You can only stop an instance if it is backed by an EBS volume. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. [Show IAM policy document](#)

☐ Terminate this instance

You will not be able to terminate this instance if termination protection is enabled. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. [Show IAM policy document](#)

☒ Reboot this instance

An instance reboot is equivalent to an operating system reboot. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. [Show IAM policy document](#)

Add EC2 action

In this EC2 action section select Reboot the instance, because whenever the cpu utilization is more than 50% the our server has to be reboot, thats the best practice.

click on next

Add name and description

Name and description

Alarm name

Alarm description - optional [View formatting guidelines](#)

Edit

Preview

This is an H1

****double asterisks will produce strong character****

This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Cancel

Previous

Next

and set an alarm name and click on next

review all the steps and click on create alarm.

Till now we configured our instance to cloud watch.

STEP-3: INCREASE THE CPU UTILIZATION MORE THAN 50%

install stress in our instance by following the commands:

- amazon-linux-extras install epel -y

- yum install stress -y

take the duplicate session of your server,

one is to monitor the cpu utilization

another one is to increase the cpu utilization

in session one use **top** command to get cpu utilization

```
top - 18:44:19 up 29 min,  2 users,  load average: 0.16, 0.10, 0.04
Tasks:  99 total,   1 running,  55 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  975600 total,  416140 free,   89100 used,  470360 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  746164 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	20	0	123620	5508	3928	S	0.0	0.6	0:02.01	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-ev
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
9	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_tasks_rude

By default my CPU ULITIZATION of my server is 0%

open the second session and use following command to increase cpu utilization

stress -c 40 -t 500 -v

-c : cpu

-t : time

-v : verbose

by this command we are giving some load to cpu, after performing the command

check the cpu utilization on 1st session again

aws

Services

Search

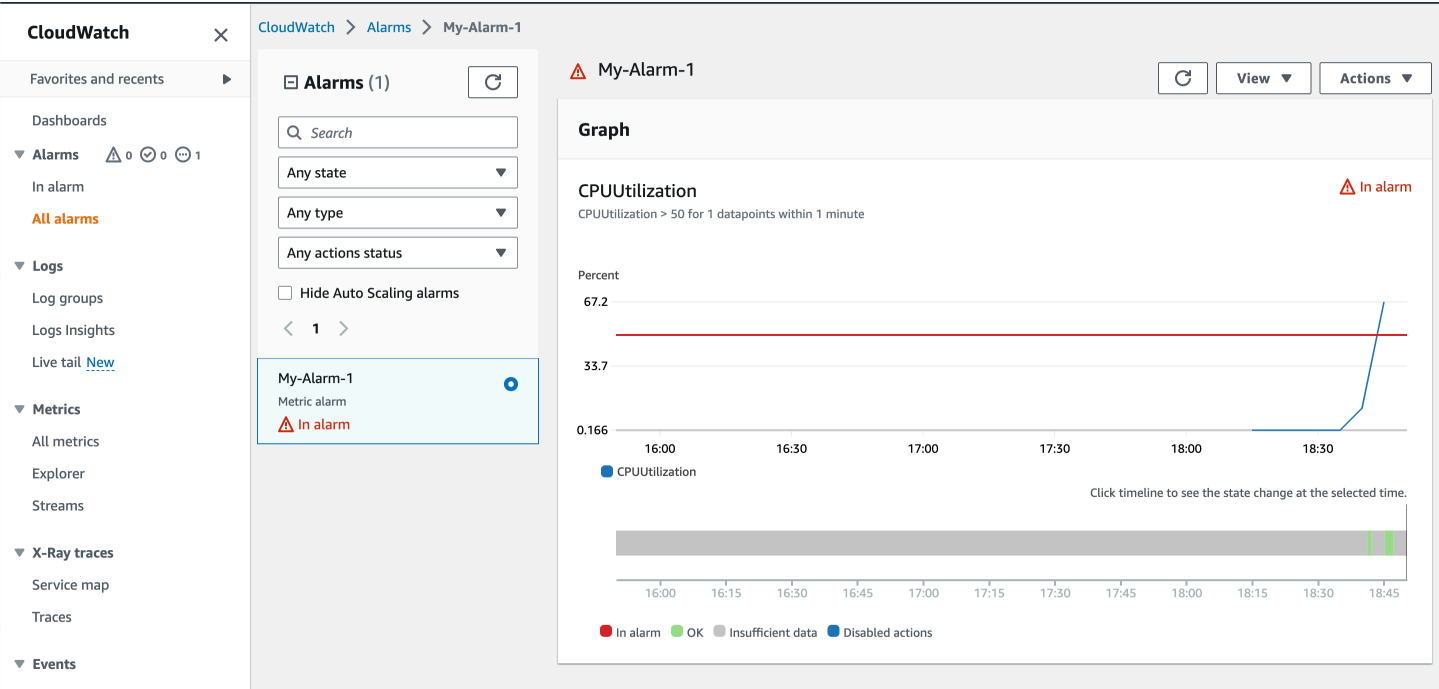
[Option+S]

```
top - 18:46:50 up 32 min, 2 users, load average: 6.16, 1.37, 0.45
Tasks: 142 total, 41 running, 58 sleeping, 0 stopped, 0 zombie
%Cpu(s):100.0 us, 0.0 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 975600 total, 407992 free, 97048 used, 470560 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 738168 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4435	root	20	0	7584	100	0	R	2.7	0.0	0:00.23	stress
4436	root	20	0	7584	100	0	R	2.7	0.0	0:00.23	stress
4437	root	20	0	7584	100	0	R	2.7	0.0	0:00.23	stress


as you can observe here my cpu reached to 100%, if it stays like this for 1 minute, then you will get mail.

meanwhile you can watch this in cloud watch also, open cloud watch and open your alarm
After waiting few minutes, by graph reached to 62% above in cloud watch



← ⓘ 🗑️ ✉️ ⌚ ↺ 📁 📄 ⋮ 2 of 272 < >

ALARM: "My-Alarm-1" in Asia Pacific (Mumbai) Inbox x 🖨️ 🔗

 **AWS Notifications** <no-reply@sns.amazonaws.com> 00:20 (0 minutes ago) ☆ ↶ ⋮
to me ▾

You are receiving this email because your Amazon CloudWatch Alarm "My-Alarm-1" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [67.23224043715847 (13/06/23 18:45:00)] was greater than the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 13 June, 2023 18:50:18 UTC".

View this alarm in the AWS Management Console:
<https://ap-south-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-south-1#alarmsV2:alarm/My-Alarm-1>

Alarm Details:

- Name: My-Alarm-1
- Description:
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [67.23224043715847 (13/06/23 18:45:00)] was greater than the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Tuesday 13 June, 2023 18:50:18 UTC
- AWS Account: 184744381800
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:184744381800:alarm:My-Alarm-1

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanThreshold 50.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:

- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-01b2538643a316ac0]
- Period: 60 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: missing

PROJECT-2: UPLOAD LOG FILES IN CLOUD WATCH

REFERENCE

(<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/QuickStartEC2Instance.html>)

STEP-1: LAUNCH EC2 INSTANCE (Ubuntu)

STEP-2: INSTALL CLOUD LOGS

DOWNLOAD FILE : curl <https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py> -O

INSTALL PYTHON : apt update && apt install python2.7 -y

RUN PYTHON FILE : python2.7 awslogs-agent-setup.py --region ap-south-1

Enter

acces_key : enter

secret_key : enter

default_region : enter

O/p_format : enter

Path to log file to upload : /var/log/apache2/access.log

Destination log group name : syslog_ec2

Log stream name: 1 (EC2 instance ID)

Log event time stamp format: 2

Initial position to upload a file : 1

More log files for configure : N

Check the service : systemctl status awslogs

vim /var/awslogs/etc/awslogs.conf —> **this is the path where we can store all the log files paths**

First lets check these files are storing in cloud watch or not, if its working fine then we can start store our app log files.

CREATE IAM ROLES:

IAM —> ROLES —> CREATE ROLE

SELECT EC2 AND ADD CLOUD WATCH PERMISSIONS

ATTACH THAT ROLE TO EC2 INSTANCE

RESTART AWS LOGS AGAIN : `systemctl restart awslogs`

Go to CLOUD WATCH AND SEE THE LOGS

CHANGE THE PATH TO OUR APP LOG FILES

To do that we have to install web server and deploy a web application

`apt install apache2 -y`

Add some files in (`/var/www/html/`)

AFTER DEPLOYED THE APPLICATION, WE HAVE TO CHECK THE APP LOGS IN (`vim /var/log/apache2/access.log` file

There you found all log info

We have to configure this path to aws cloud watch logs

TO DO THAT

Go to the path : `vim /var/awslogs/etc/awslogs.conf`

Go to the last line of the file and copy the data as it is (change path)

RESTART CLOUDWATCH LOGS : `systemctl restart awslogs`

RESTART WEBSERVER : `systemctl restart apache2`

RELATIONAL DATABASE SERVICE

Usually we have 2 types of databases

Relational databases : Oracle, MYSQL, PostgreSQL etc...

No-SQL databases : Mongo DB, Dynamo DB etc..

IN RD → we store the data in table format

In early days we have to purchase the databases like

Buy database license

Set up machines to install db server

Set database server

setup network, power and AC connections

Setup security resources

Setup data backups

But now a days most of the companies are moving to cloud, if your choice is AWS

They will take care each and everything about these databases and maintenance

We just need to create a database and relax

HOW TO CREATE RDS :

Go to RDS in AWS Console

**Consider creating a Blue/Green Deployment to minimize downtime during upgrades**

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

**Databases (0)**☒ Group resources

Modify

Actions ▾

Restore from S3

Create database

< 1 > ⚙

DB identifier ▲	Status ▾	Role ▾	Engine ▾	Region & AZ ▾	Size ▾	Actions ▾	CPU ▾	Current activity ▾
-----------------	----------	--------	----------	---------------	--------	-----------	-------	--------------------

No instances found

Click on Create database

Create database

Choose a database creation method [Info](#)**Standard create**

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

**Easy create**

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Select Standard Create

Engine options

Engine type [Info](#)

☐ Aurora (MySQL Compatible)



☐ Aurora (PostgreSQL Compatible)



☒ MySQL



☐ MariaDB



☐ PostgreSQL



☐ Oracle

ORACLE®

☐ Microsoft SQL Server



Select MySQL Engine

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings



Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter.

☐ **Manage master credentials in AWS Secrets Manager**

Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

 If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.
[Learn more](#) 

☐ **Auto generate a password**

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

In this settings give database name and set database password

username: admin

password: mypassword

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.



Amazon RDS Optimized Writes - *new* [Info](#)



Show instance classes that support Amazon RDS Optimized Writes

DB instance class [Info](#)

- ☐ Standard classes (includes m classes)
- ☐ Memory optimized classes (includes r and x classes)
- ☒ Burstable classes (includes t classes)

db.t2.micro

1 vCPUs 1 GiB RAM Not EBS Optimized



Include previous generation classes

In this instance configuration step select db.t2.micro which is completely free tier

Storage

Storage type [Info](#)

General Purpose SSD (gp2)

Baseline performance determined by volume size



Allocated storage [Info](#)

20

GiB

The minimum value is 20 GiB and the maximum value is 6,144 GiB

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

☐ Enable storage autoscaling

Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

In this storage section give 20 GB of SSD and disable autoscaling



Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

- ☒ **Don't connect to an EC2 compute resource**
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

- ☐ **Connect to an EC2 compute resource**
Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

Default VPC (vpc-0fdfa5015fd4b4f2d)

3 Subnets, 3 Availability Zones



Only VPCs with a corresponding DB subnet group are listed.

- After a database is created, you can't change its VPC.

DB subnet group [Info](#)

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

default



Public access [Info](#)

- ☐ **Yes**
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.
- ☒ **No**
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

In this connectivity part, Since i don't have any EC2 instances so i am not going to connect my servers,

VPC and Subnets will be default

Public access will be NO

VPC security group (firewall) [Info](#)

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☐ Choose existing
Choose existing VPC security groups

☒ Create new
Create new VPC security group

New VPC security group name

MY-RDS

Availability Zone [Info](#)

No preference ▼

RDS Proxy

RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.

☐ Create an RDS Proxy [Info](#)
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

Certificate authority - optional [Info](#)

Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

rds-ca-2019 (default) ▼

If you don't select a certificate authority, RDS chooses one for you.

► Additional configuration

Security groups : it will create a new Sg for me and then i will change it to later as per my requirement.

Database authentication

Database authentication options [Info](#)

- ☐ Password authentication
Authenticates using database passwords.
- ☒ Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.
- ☐ Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Here we have to select Password and IAM database authentication

Estimated Monthly costs

DB instance	17.52 USD
Storage	2.62 USD
Total	20.14 USD

This billing estimate is based on on-demand usage as described in [Amazon RDS Pricing](#). Estimate does not include costs for backup storage, IOs (if applicable), or data transfer.

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#).

And this is the monthly billing, but dont worry about this because we are using only less than one hour, so we will not get billing much may be 5-6 rs

Finally click on create database it will take atleast 5 minutes to create our database.

Successfully created database database-1

View connection details

You can use settings from database-1 to simplify configuration of [suggested database add-ons](#) while we finish creating your DB for you.

How was your experience creating an Amazon RDS database? [Provide feedback](#)

RDS > Databases

Consider creating a Blue/Green Deployment to minimize downtime during upgrades

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

Databases (1)

☒ Group resources

Modify

Actions

Restore from S3

Create database

	DB identifier	Status	Role	Engine	Region & AZ	Size	Actions	CPU	Current activity	Maintenance
	database-1	Backing-up	Instance	MySQL Community	ap-south-1a	db.t2.micro	-	-		none

Finally my Database is created.

Connectivity & security	Monitoring	Logs & events	Configuration	Maintenance & backups	Tags
Connectivity & security					
Endpoint & port Endpoint database-1.crrlrczntuiv.ap-south-1.rds.amazonaws.com Port 3306	Networking Availability Zone ap-south-1a VPC vpc-0fdfa5015fd4b4f2d Subnet group default-vpc-0fdfa5015fd4b4f2d Subnets subnet-02fc7def13e25e72b subnet-0f46aa59e7790fd46 subnet-0c21e0811c704223f Network type IPv4		Security VPC security groups MY-RDS (sg-07e302ad2d7234bbf) Active Publicly accessible No Certificate authority Info rds-ca-2019 Certificate authority date August 22, 2024, 22:38 (UTC+05:30) DB instance certificate expiration date August 22, 2024, 22:38 (UTC+05:30)		

This is details of my database

LAUNCH AN INSTANCE IN SAME VPC (where our DB is created)

INSTALL MYSQL:

- `sudo rpm -Uvh https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm`
- `rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022`
- `sudo yum install mysql-community-server -y`
- `sudo systemctl enable mysqld`
- `sudo systemctl start mysqld`
- `sudo grep 'temporary password' /var/log/mysqld.log`
- `sudo mysql_secure_installation`

TO CONNECT WITH DATABASE

- Modify the security groups :

Go to security groups >> select MY-RDS security groups and click on edit inbound rules >>>

Add rule >> MySql/Aurora

source : our-instance-sg (MY-SG)

Edit inbound rules [Info](#)

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

Inbound rules [Info](#)

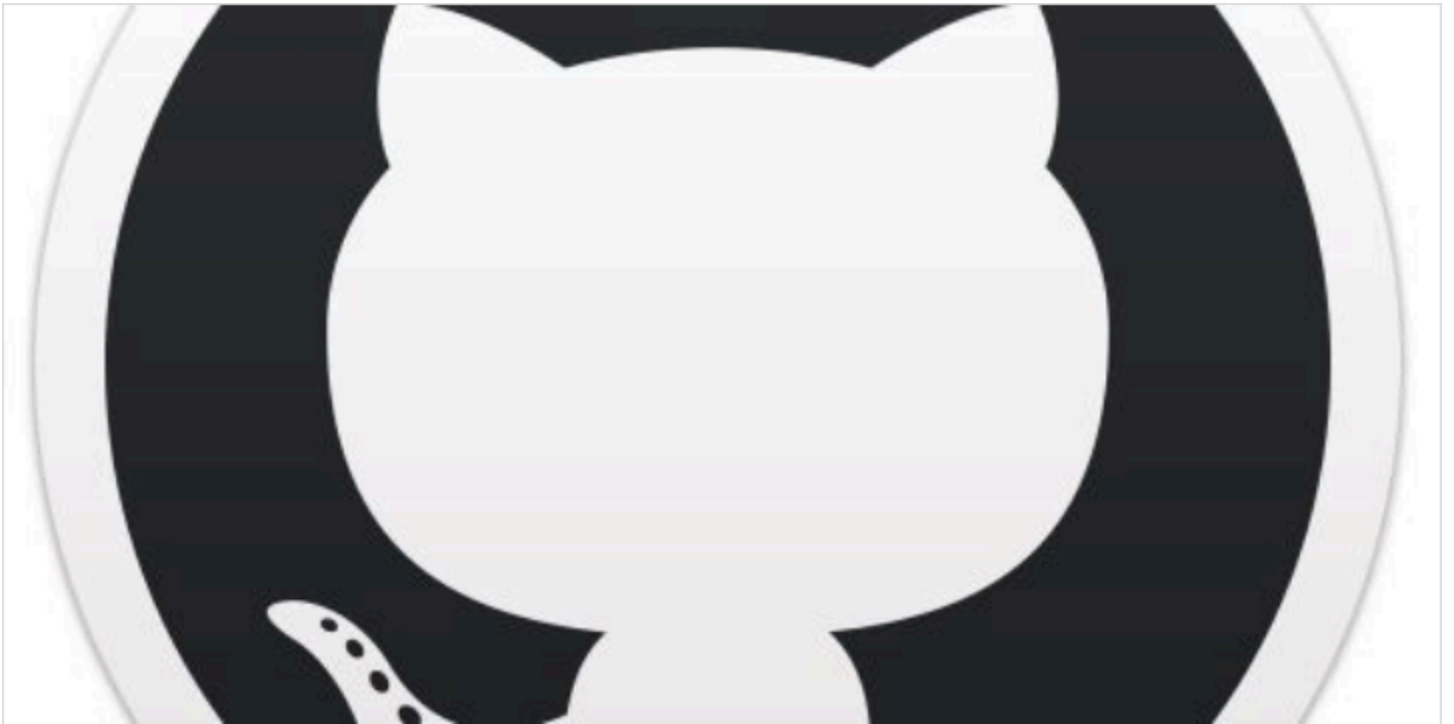
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info		
sgr-0a26a12f0cea1aded	MySQL/Aurora ▼	TCP	3306	Custom ▼	<input type="text" value="Q"/>	<input type="text"/>	<input type="button" value="Delete"/>
				<div> <div>sg-01c5bac7d17874d7b</div> <div>✕</div> </div>			
sgr-01891400b7126bfcd	MySQL/Aurora ▼	TCP	3306	Custom ▼	<input type="text" value="Q"/>	<input type="text"/>	<input type="button" value="Delete"/>
				<div> <div>49.205.248.195/32</div> <div>✕</div> </div>			

click on save now

This means we are adding our SG to DATABASE SG

- perform command to connect with database : **mysql -h endpoint -u username -p**
- It will asks you password enter it and you will connect with database.
- after connecting with mysql, perform some database commands
 - **show databases;** ---> to show the list of databases
 - **CREATE DATABASE accounts;** -----> this command is used to create a database

INSTALL GIT AND GET A SOURCE CODE



go to **/root/docker-webapp/src/main/resources**

You will find a database schema/query (db_backup.sql) that you have to deploy on database.

command: **mysql -h endpoint -u user -p database_name < db_backup.sql**

enter the password

Login into database: **mysql -h endpoint -u user -p**

use accounts; -----> To change to accounts database

show tables; -----> To see list of tables in accounts database

exit from the database

INSTALL MAVEN & STEUP TOMCAT

To build and deploy the source code

give mvn clean package to get war file

copy the war file to webapps folder in tomcat

THE APPLICATION IS DEPLOYED INTO TOMCAT

TRY TO CREATE AN ACCOUNT INTO THE APPLICATION YOU WILL GET HTTP 500 ERROR

TO RESOLVE THOS WE NEED TO CONNECT DATABASE TO OUR APPLICATION.

To do that : vim apache-tomcat-9.0.76/webapps/vprofile-v2/WEB-INF/classes/application.properties

change the details as

username : admin

password : mypassword

endpoint : database-1.ccrirczntuiv.ap-south-1.rds.amazonaws.com

jdbc.url=jdbc:mysql://**database-1.ccrirczntuiv.ap-south-1.rds.amazonaws.com:3306/accounts?useUnicode=true&characterEncoding=UTF-8&zeroDateTimeBehavior=convertToNull**

jdbc.username=**admin**

jdbc.password=**mypassword**

RESTART TOMCAT AND USE APPLICATION