AWS CloudWatch & SNS

What’s CloudWatch and SNS (Simple Notification Service)

Assume we have an application on EC2 ---> if something goes wrong in the application, how will you monitor that? You could set some kind of an alarm. Once this alarm is triggered, on your phone or mail, you will get this notification. If something goes wrong, immediately I want to trigger an alarm. I want to trigger if utilization of CPU > 50%. From triggering alarm, I want to publish into a service called as SNS. Using SNS, I will be sending email or sms to inbox. If something went wrong, I will trigger an alarm, based on what’s happening, I will publish in SNS. In SNS, I will configure such that to get an email or SMS

Email

SNS

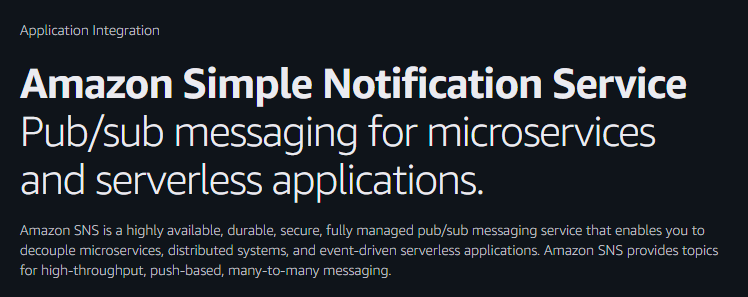
Alarm

EC2

Subscribe to that topic

Publish onto SNS

APP



Publishing means sending that message, Subscribing means getting that message.

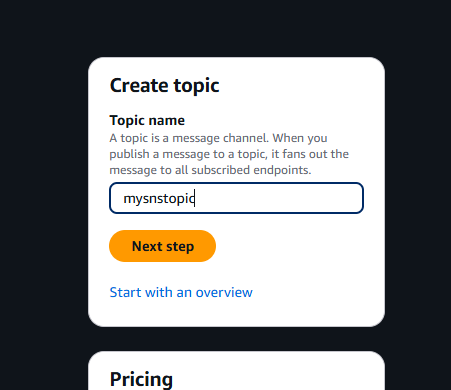
Netflix is publishing the movies, we subscribe to Netflix to get those movies

We need to create a topic in SNS --> onto that topic we will publish what as gone wrong from the monitoring ---> subscribe to that topic --> send that event via an email.

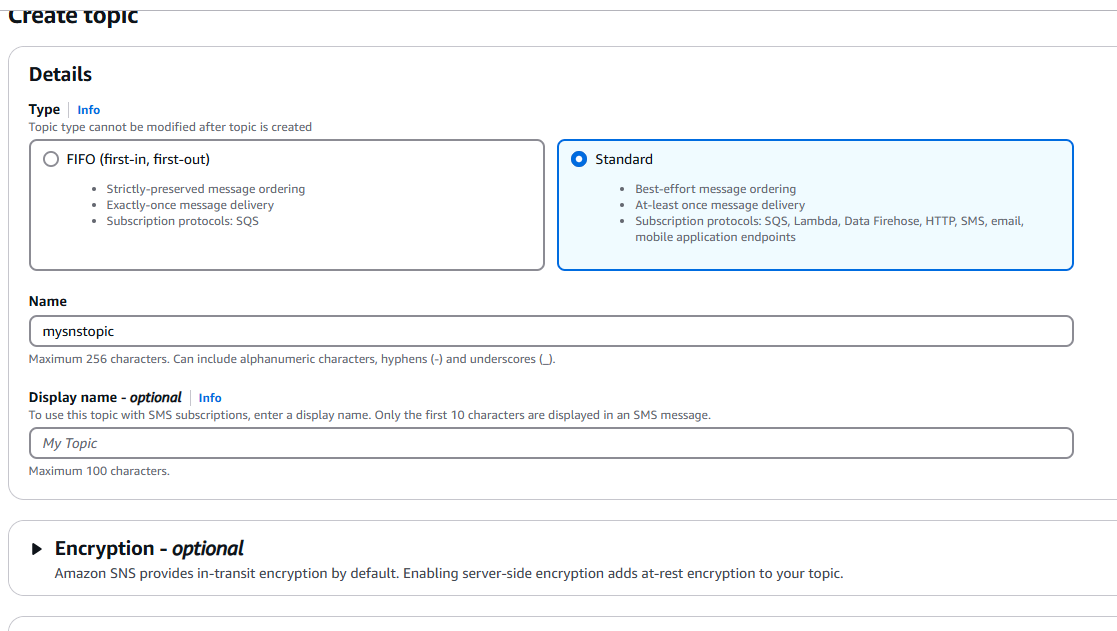
Summary:

Amazon CloudWatch is a component of AWS that provides monitoring of AWS resources and the customer applications running on AWS infrastructure. It enables real-time monitoring of AWS resources like EC2 instances, Elastic block store, Load balancers, RDS, etc

The application automatically collects and provides metrics for latency, request counts, CPU utilization

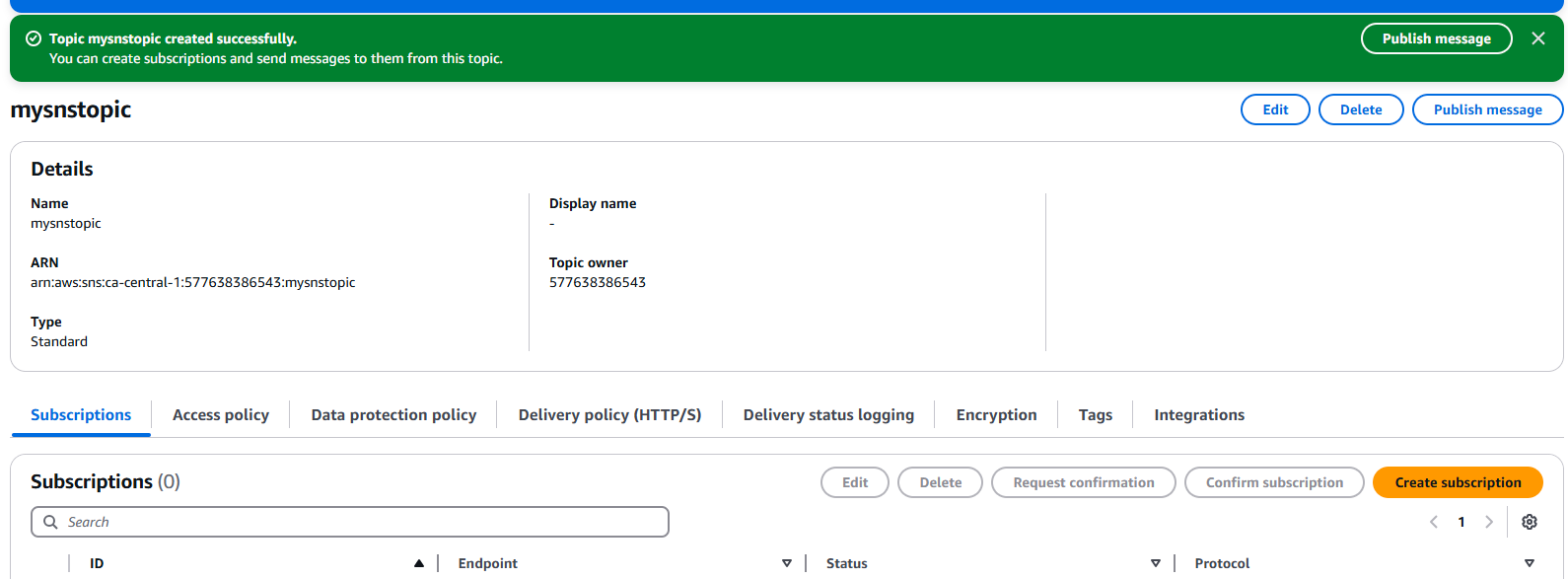


Select Standard

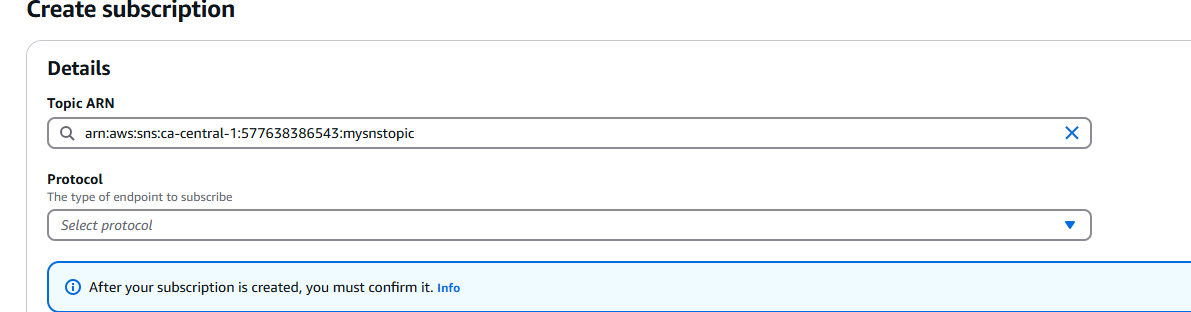


Click Create Topic

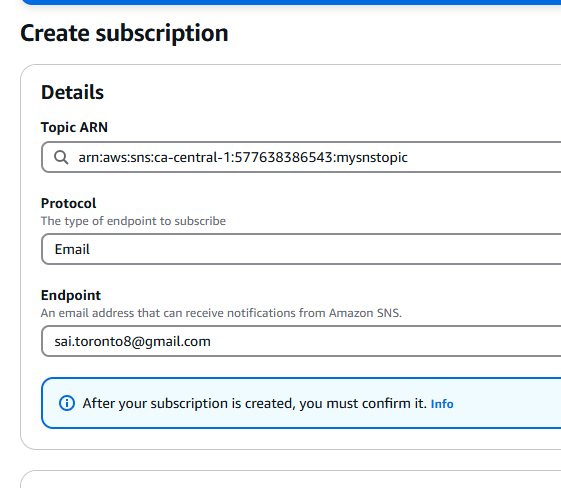
Then click Create Subscription



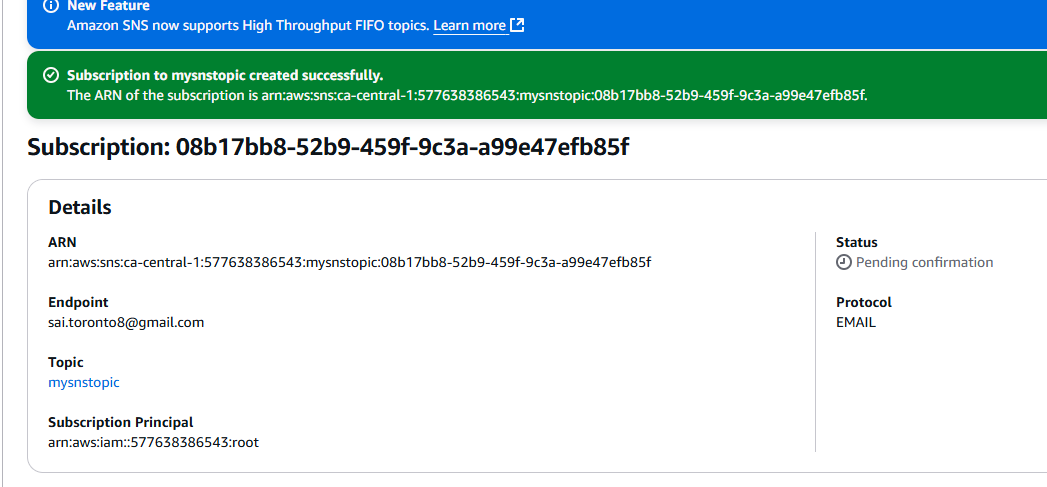
Protocol select Email



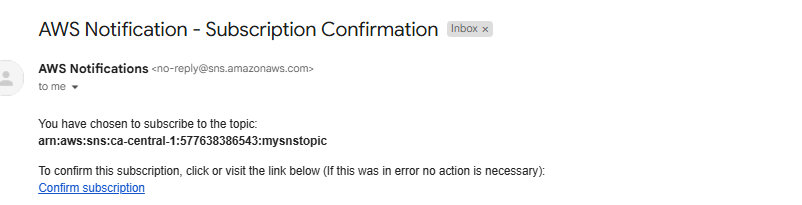
Enter Email

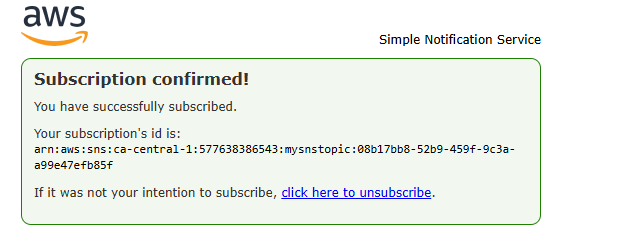


Click Create Subscription

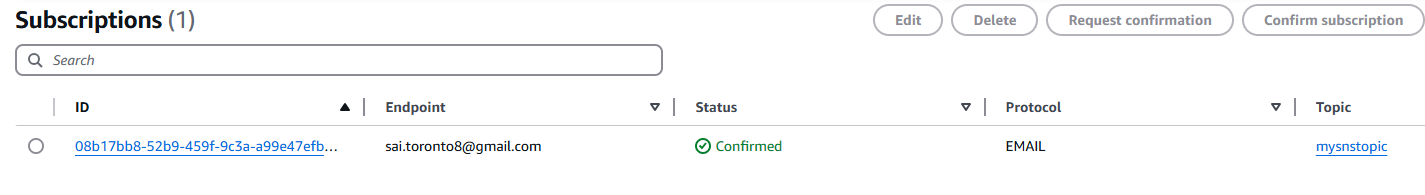


Go to Email and confirm subscription

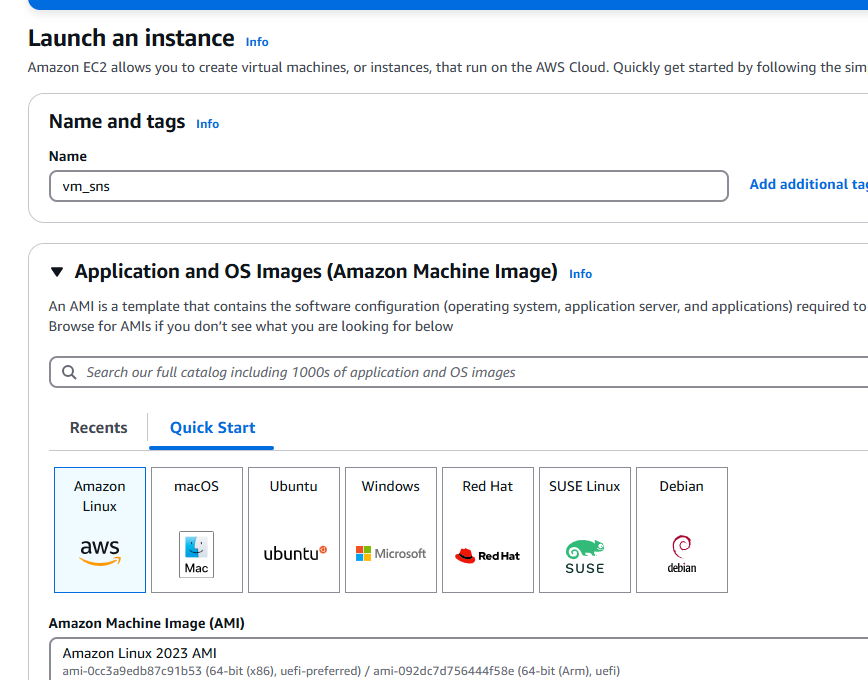




We have one subscription and it is confirmed

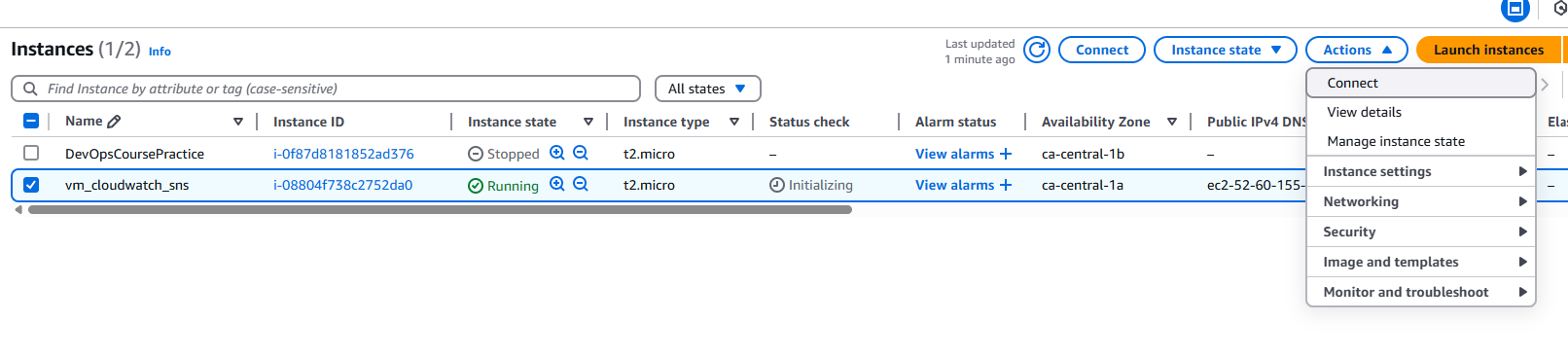


Go to EC2 and create an instance

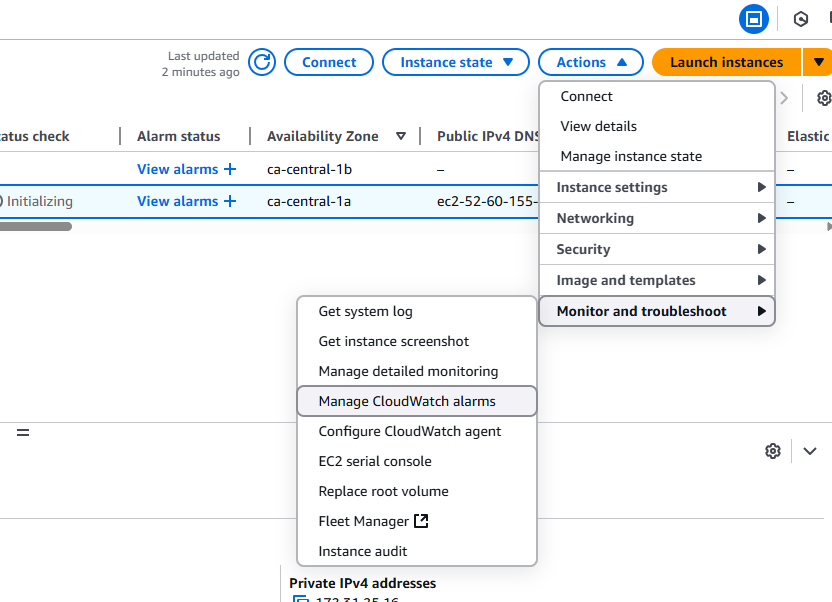




Select instance ---> Actions ---> Monitor and Troubleshoot

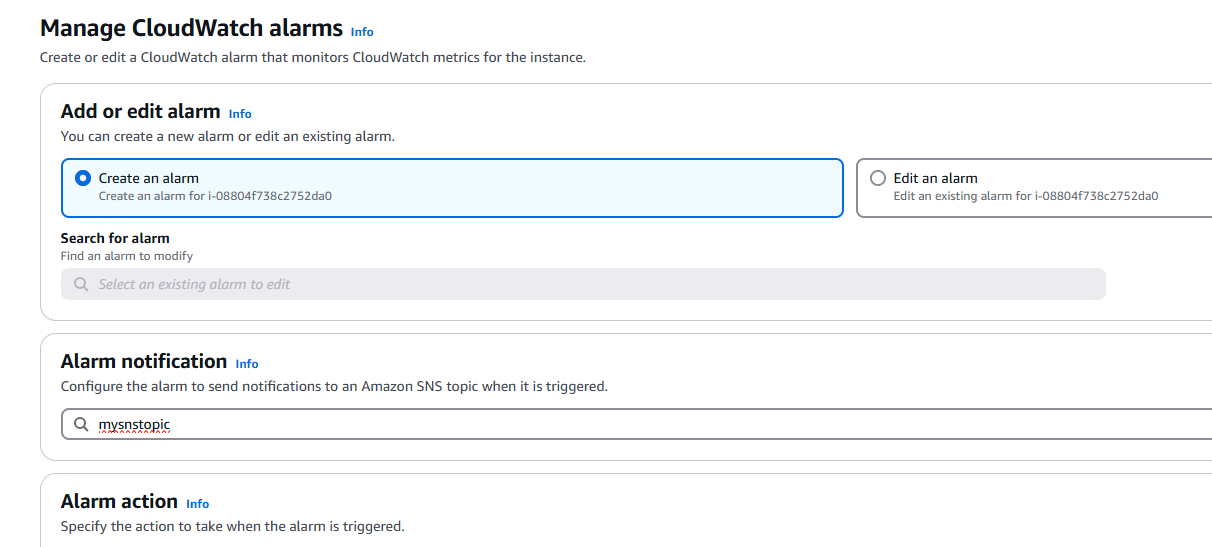


Select Manage CloudWatch alarms

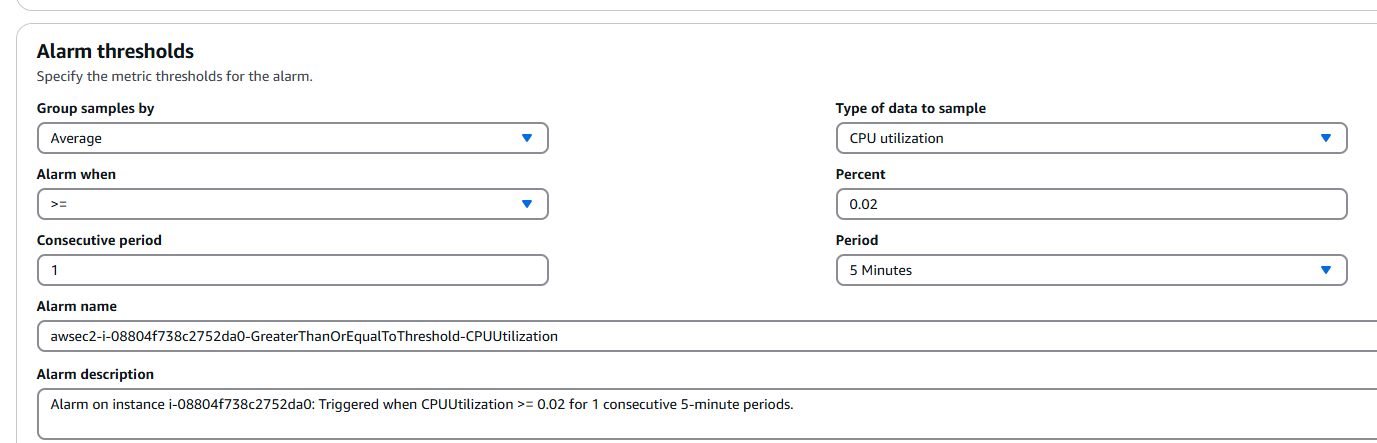


Create an alarm

Select my SNS topic here: mysnstopic



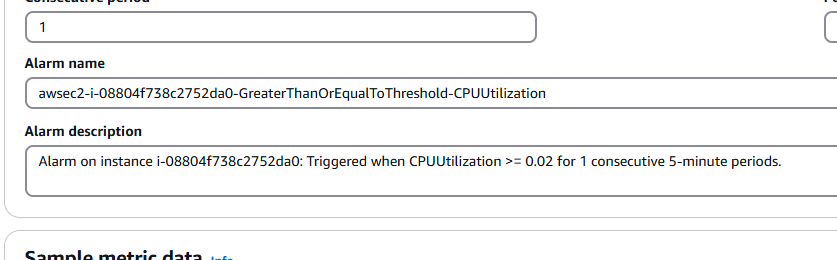
When load is > 2%, trigger this alarm



What do you want to do if alarm is triggered?

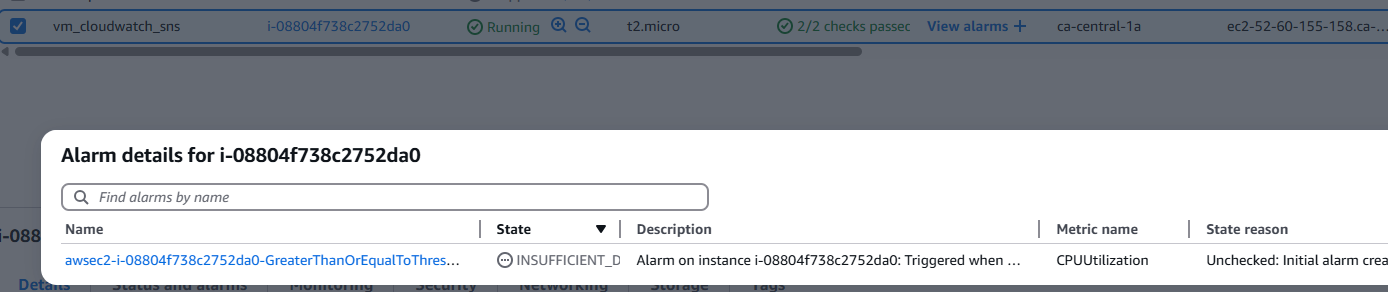
Stop, Terminate, Reboot EC2?



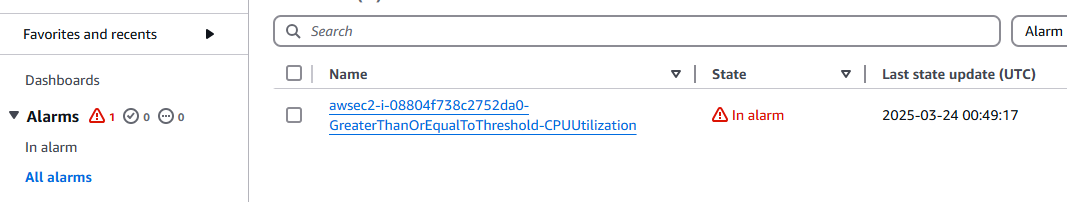


Select Create

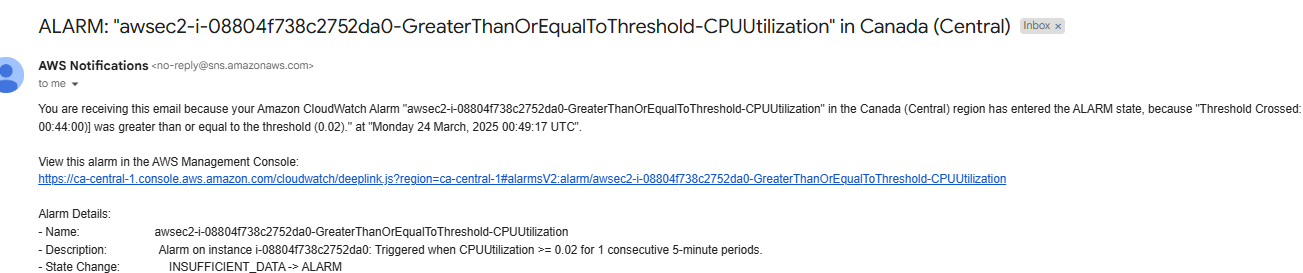
Click on EC2 instance, View alarms



Go to CloudWatch, click All alarms



Go to email and check the Alarm report



Summary:

1. Create SNS topic with Email notification (Standard create)
2. Configure Email subscription in SNS topic (We have to confirm subscription received in email)
3. To demonstrate, we have taken EC2 resource so create EC2 VM after which Select EC2 instance ---> Action ---> Monitor and troubleshoot ---> Manage CloudWatch alarms ---> Create CloudWatch alarm
4. Alarm notification : Select SNS topic which we have created
5. Alarm Threshold: AVG CPU >= 2%
6. Try to connect to VM and increase the load
7. Observe the behavior of CloudWatch / SNS (We should be getting an Email notification)
8. When alarm is triggered its status will change to “In Alarm” in CloudWatch

If you want to monitor Alarm history --> Select Alarm --> Click Alarm --> Click on History

We are able to access AWS Cloud from Web console

AWS CLI

AWS Cloud

Web console (GUI)

Terraform

AWS SDK

For DevOps Engineer, which option is trending in industry, it is Terraform

AWS CLI: Command-line interface

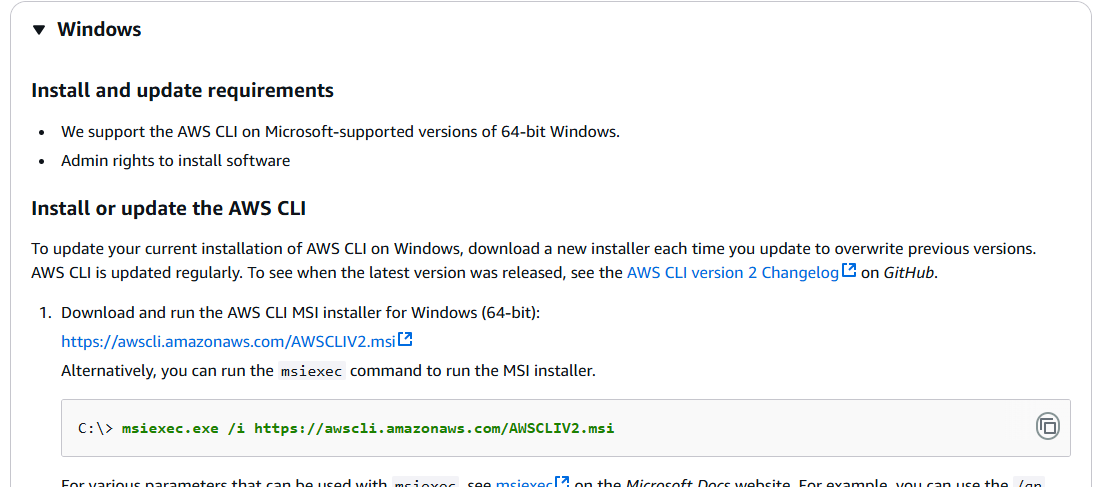
Ways for infrastructure configuration: AWS management web console, AWS CLI (Command-Line Interface)

AWS CLI ---> Usually the script provides you with flexibility to manage AWS resources and infrastructure

We need an AccessKey and SecretKey

Go to : <https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>

Click on this link:

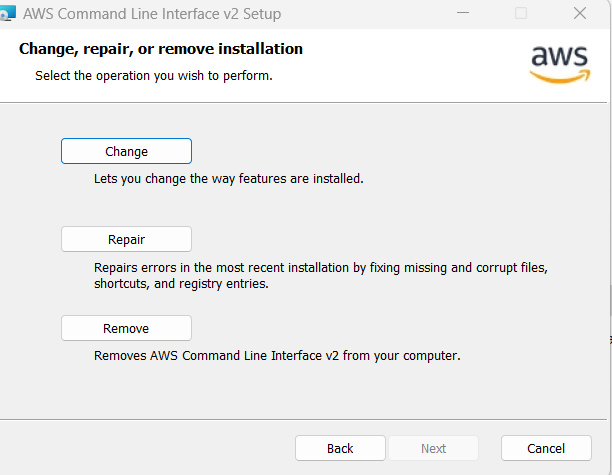


Install AWS CLI on Windows

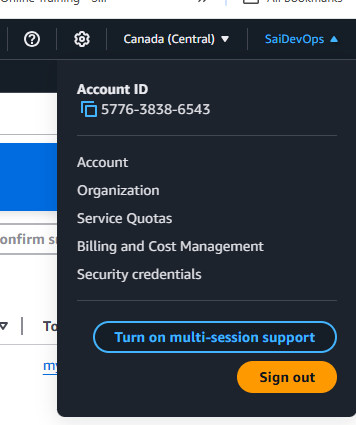
msiexec.exe /i <https://awscli.amazonaws.com/AWSCLIV2.msi>

Or click on [https://awscli.amazonaws.com/AWSCLIV2.msi](https://awscli.amazonaws.com/AWSCLIV2.msi" \t "https://docs.aws.amazon.com/cli/latest/userguide/_blank)

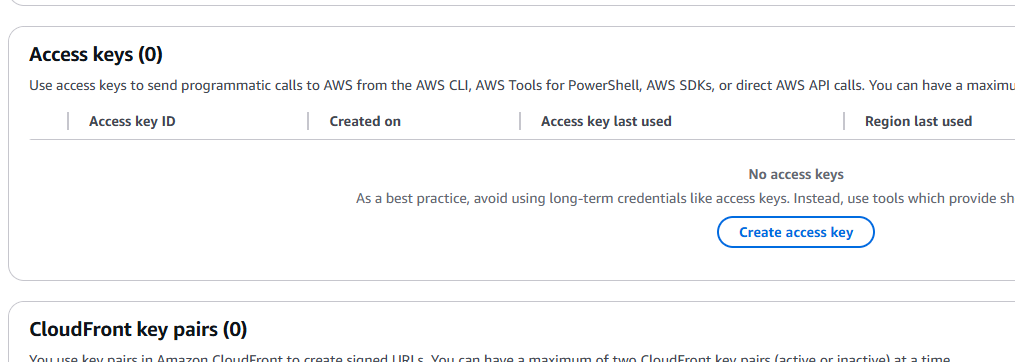
Install AWS CLI



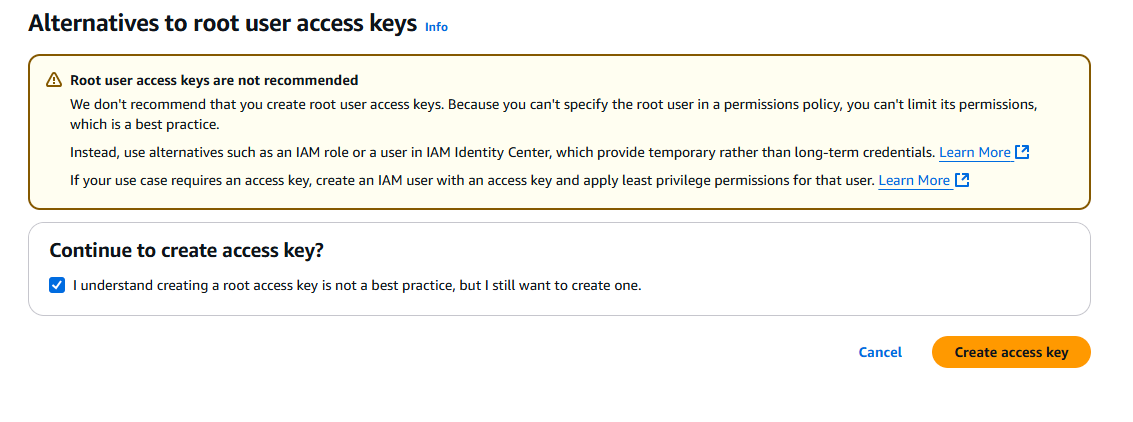
Go to AWS Console ---> Security credentials



Create access key --> What’s recommended is. Create an IAM user first then create access key for that IAM user

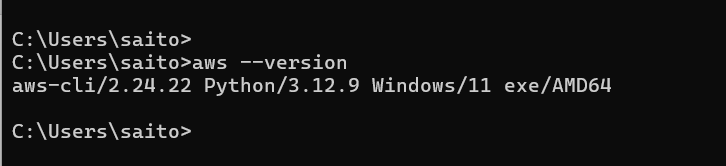


I will delete access key right after using it



Configuring AWS CLI

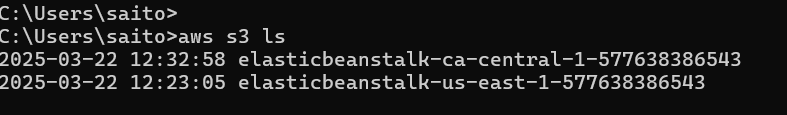
1. Create an AWS account in order to configure AWS CLI (Use existing if you already have one)
2. Create IAM user with Security credentials (Access key and Secret key)
3. Open Command prompt and connect



Next type --> aws configure

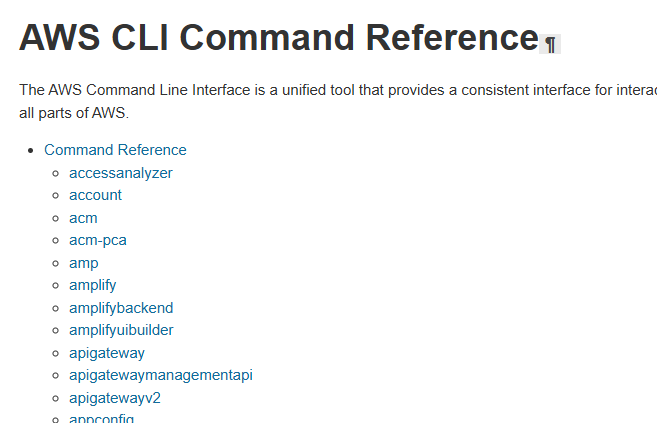
Enter AWS Access key and secret key

Correct the region to ca-central-1



Go to AWS CLI Command Reference

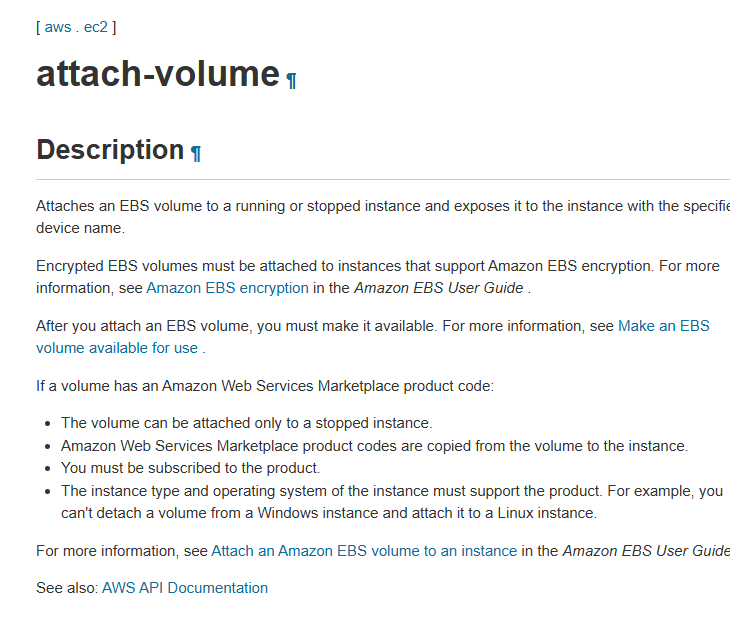
<https://docs.aws.amazon.com/cli/latest/>

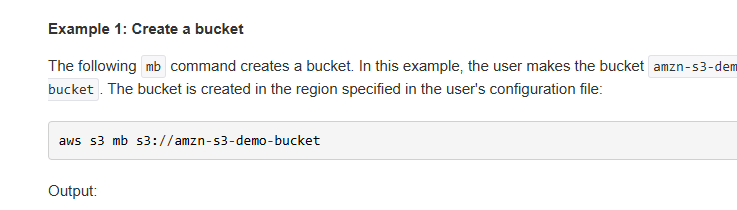


CLI Documentation: <https://docs.aws.amazon.com/cli/latest/>

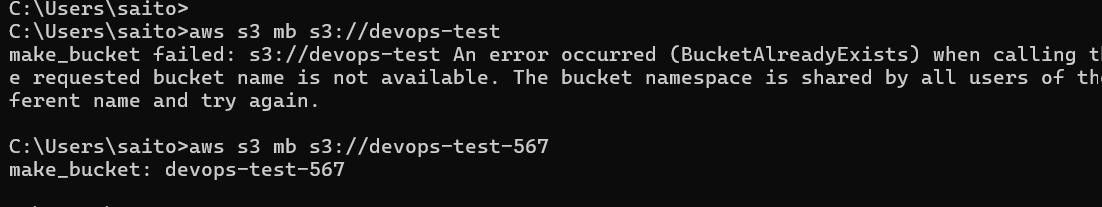
Example for EC2: <https://docs.aws.amazon.com/cli/latest/reference/ec2/>

Example to attach volume to EC2

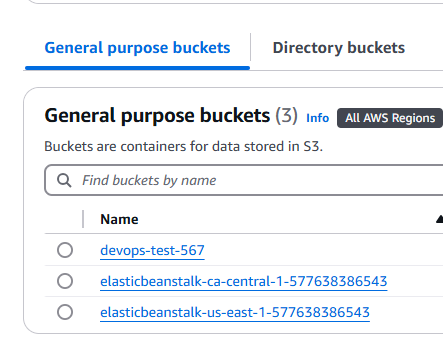


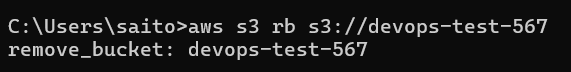


Create a new bucket



One more bucket is there





For every action we need to use commands and which command to run those details are available in AWS documentation

For example:

To Display bucket list: aws s3 ls

Create a new bucket: aws mb s3://<new\_bucket>

Delete an empty bucket: aws rb s3://<bucket\_name>

