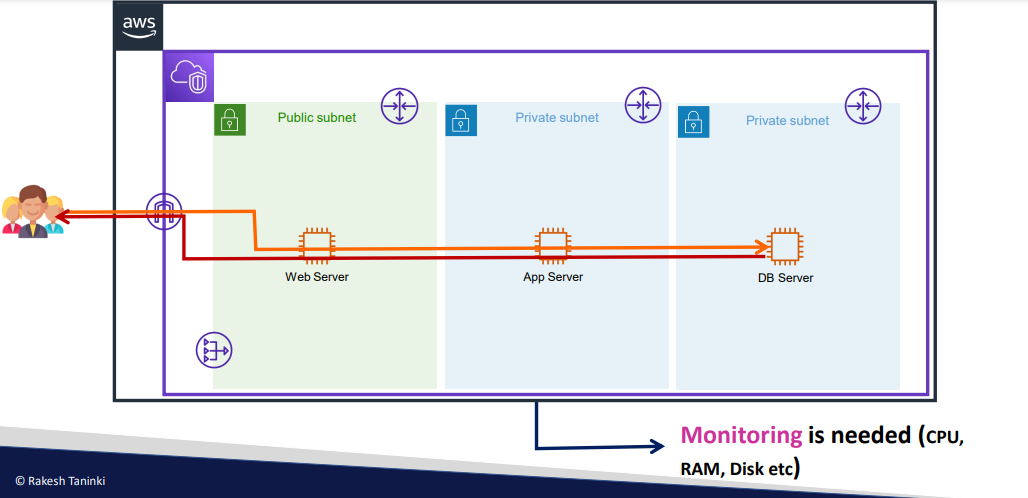
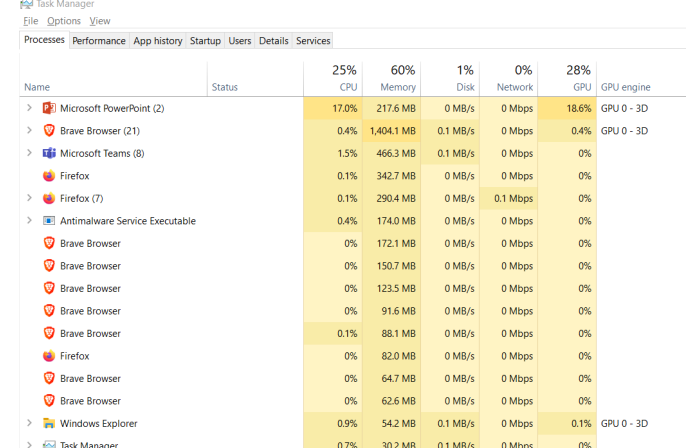
**Cloud Watch** : Resource Monitoring like how much cpu is utilized, how much ram is utilized , how much storage is utilized etc etc

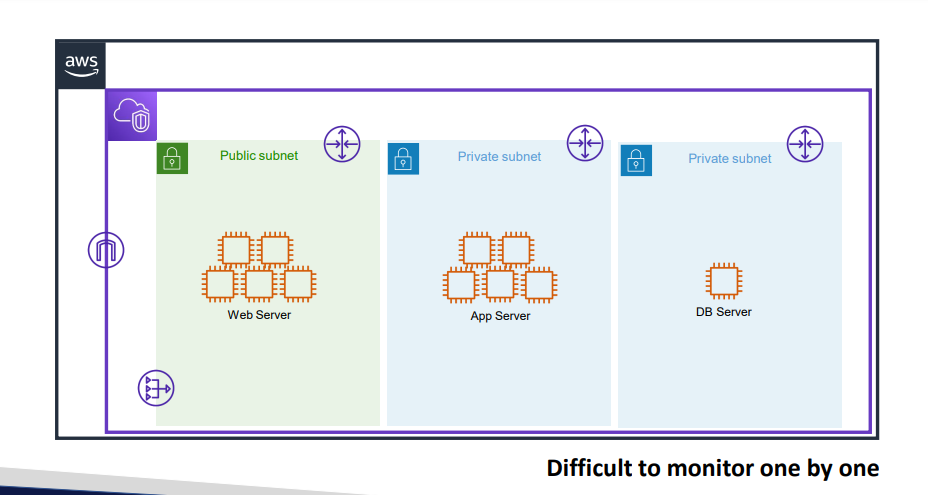
**Cloud trial** : Its account level for example if we have many users in account cloud trail specifies who created ec2 instance , who has deleted that instance etc etc



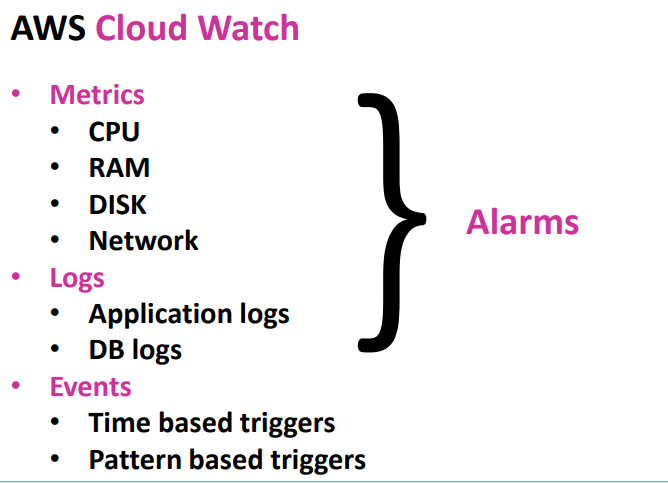
Cpu ,ram,disk is known as metrics information

* In real time we have multiple servers so we cant login to each act and check this utilization info
* So we use cloud watch to resolve this issue
* Cloudwatch,nagios,datadog etc etc are the tools which we use to monitor the resources
* 

In windows we have task manager to see the performance dashboard



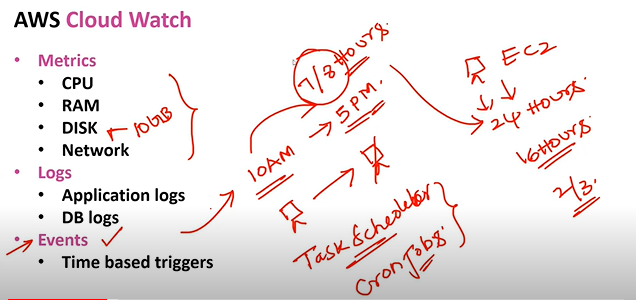
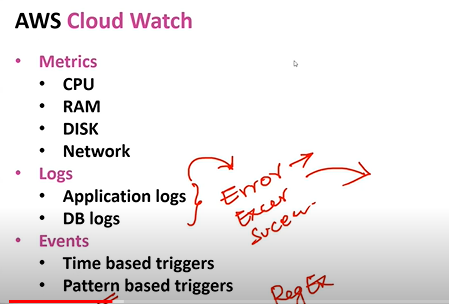
* In aws we have cloud watch
* 
* So directly if use other than aws tools like nagios etc etc for metrics monitoring we need Software called agent which pushes metrics info from aws to dashboard
* Even in cloudwatch we need agent for advanced metrics
* Without agent it only gives some metrics



Logs : if there is any error who is running that application currently those kind of info will be stored in logs even for logs we need to have agent… we can the data storage ho long it needs to store

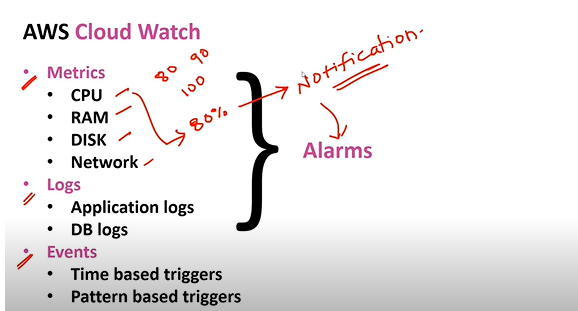
* Events if your server wants to run in only specific time like ur business hours are 10 am -5pm u r server should run only at that specific time that would be beneficial for saving purpose

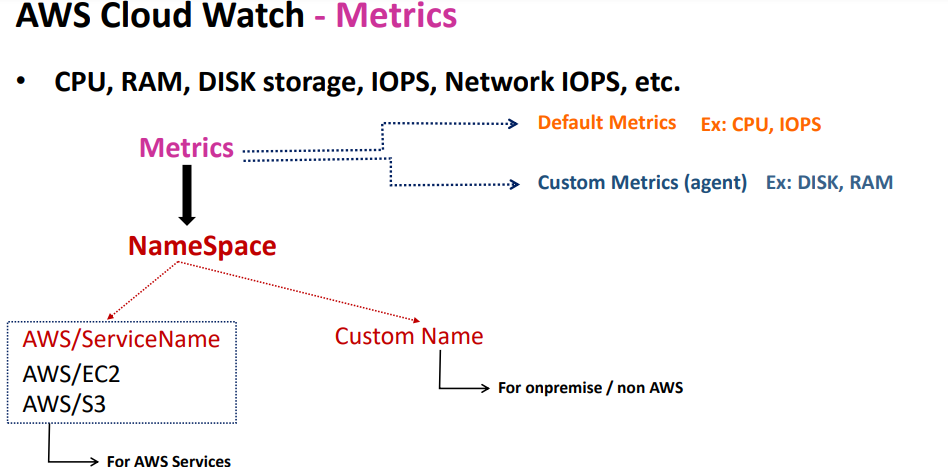
That we can create in events for automation

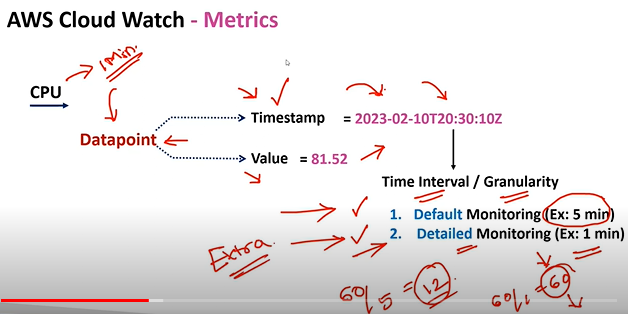
* In windows we use task scheduler and in linux we use cron jobs for job automation in aws we events
* 
* 

Time based triggers : u are setting some time to run the jobs

**Pattern based triggers** are for ex we have logs and we get error in applications at that time developers need get triggered immediately so we need to set pattern based

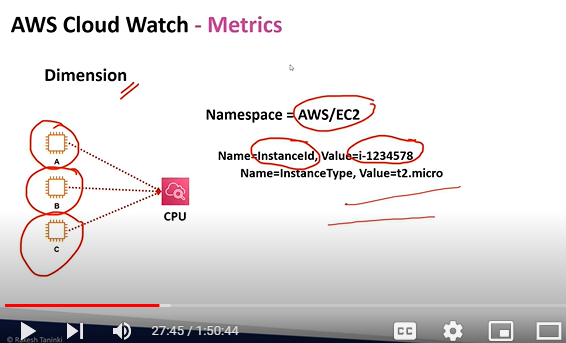


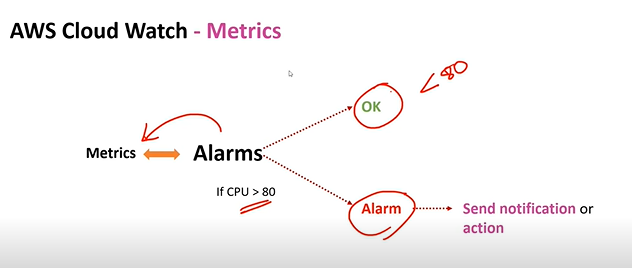
* Using alarms we can get notifications if metrics performance gets exceeded
* 
* For every metrics we need to create namespace

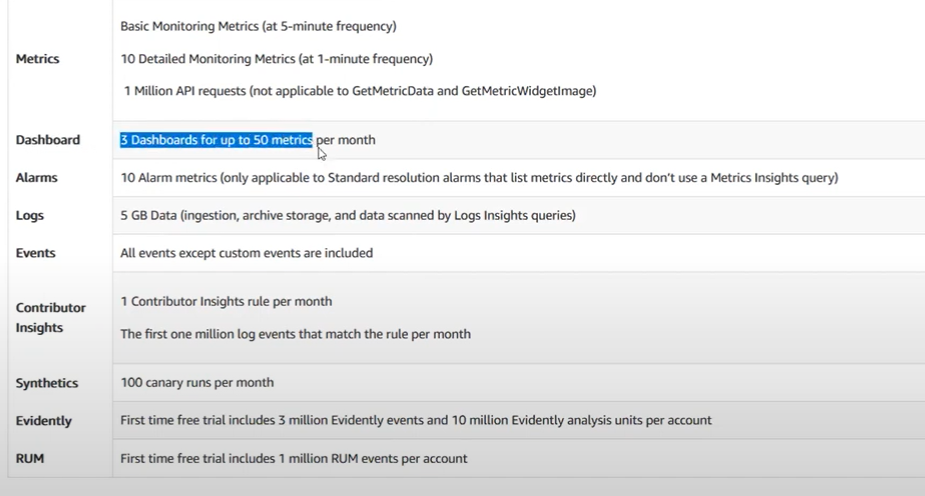


In detailed monitoring aws charges extra amount when compare to default monitoring

* In datapoints we are only getting performance but ifwe want to know for which server metrics is high then in dimentions we can get that data



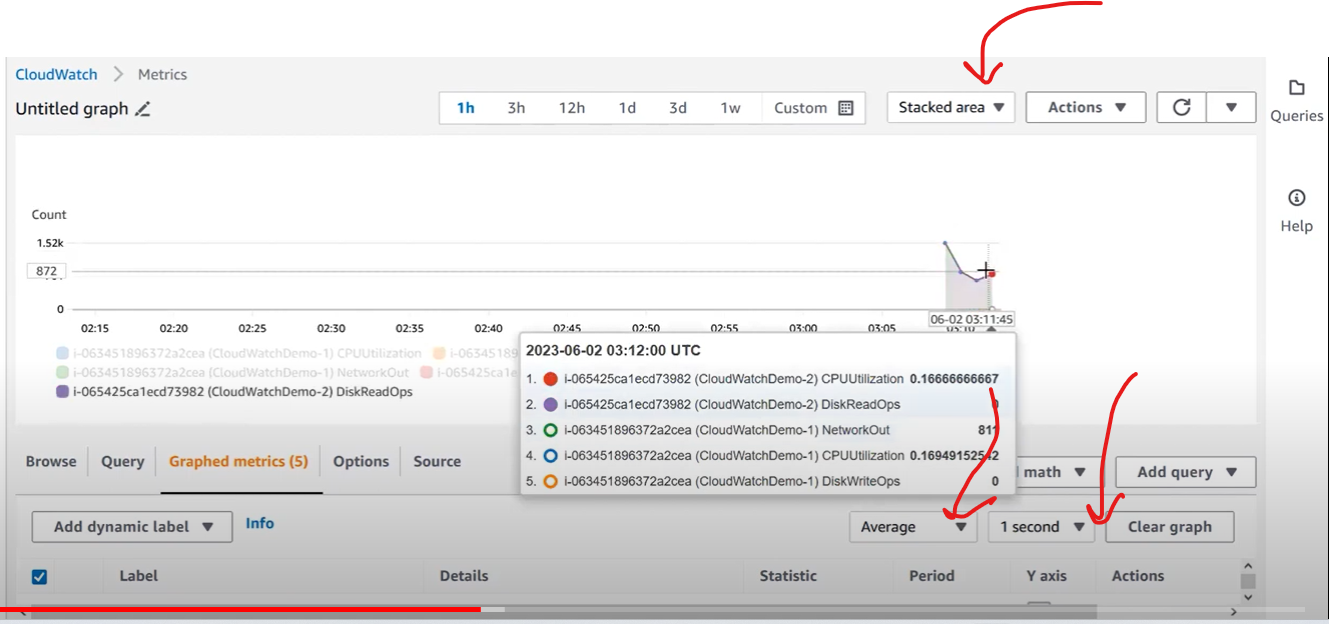




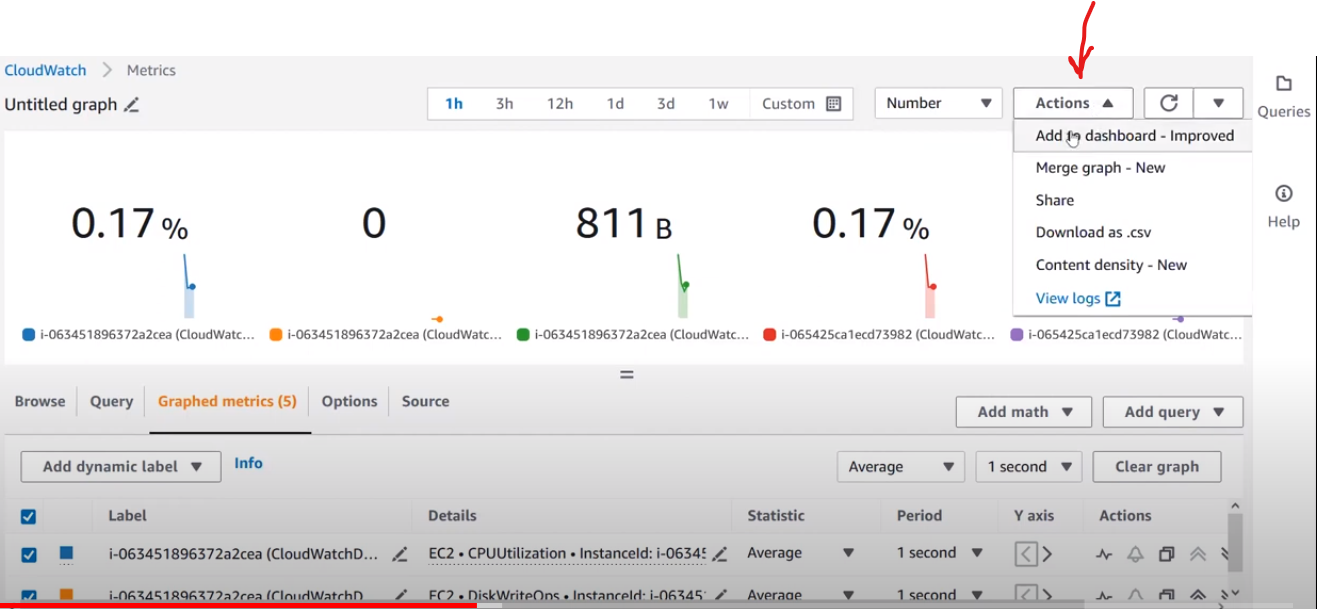
**DEMO:**

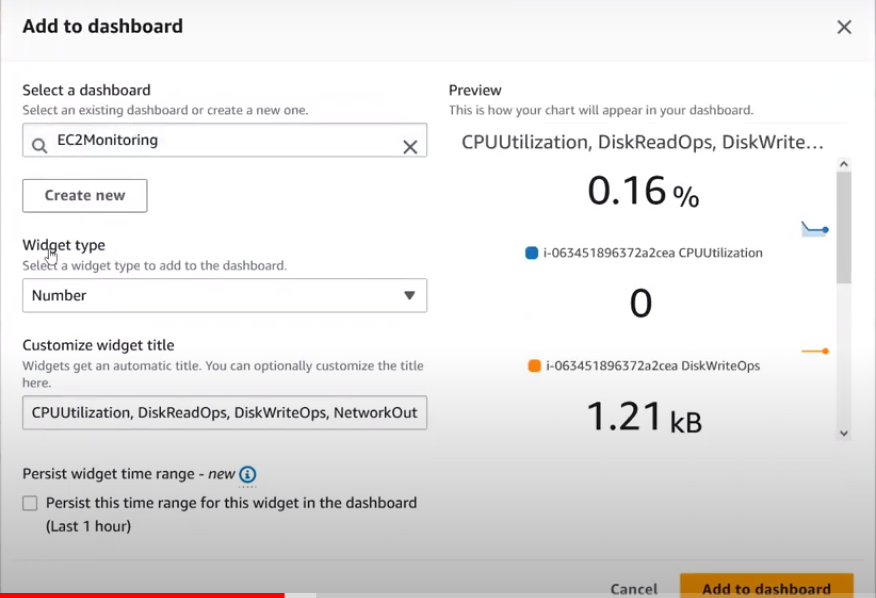
**1: STEP 1 CREATE EC2 SERVERS WITH DETAILED MONITORING ENABLE**

**2: Check the metrics in cloudwatch service for the instance you have created by instance id**

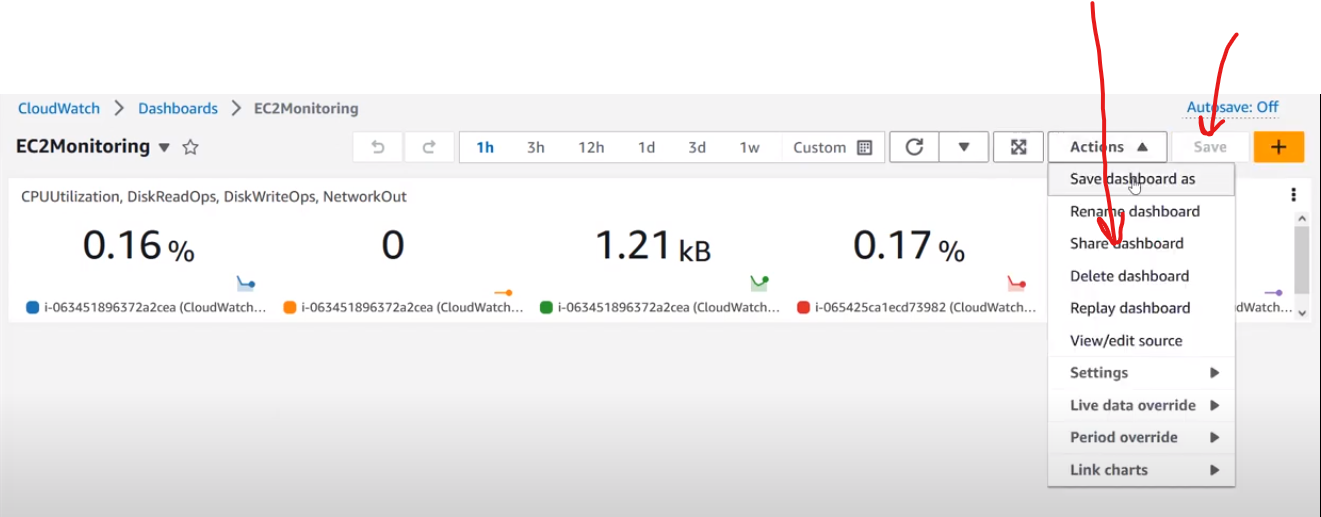
****

**If you want to create a dashboard**

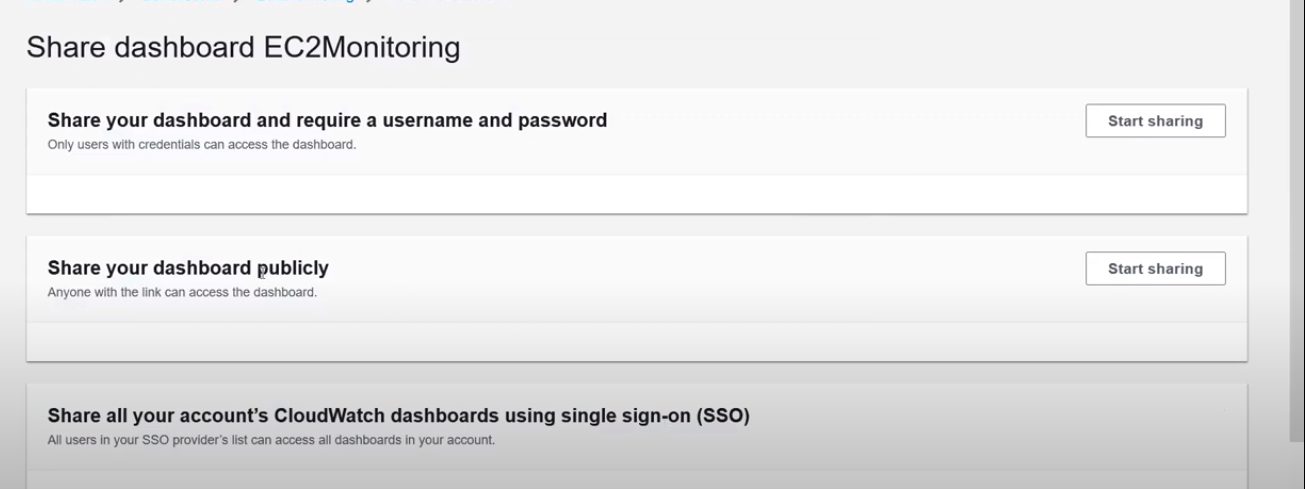
****



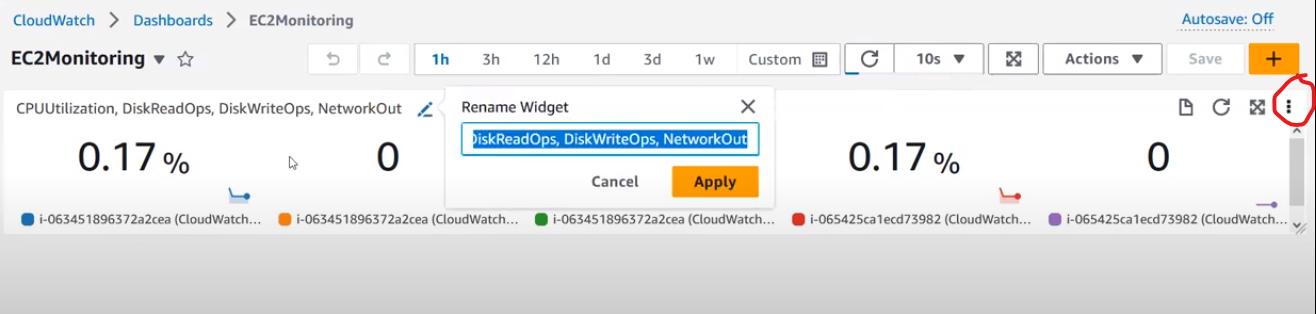
If you want to share the dashboard click on save and share



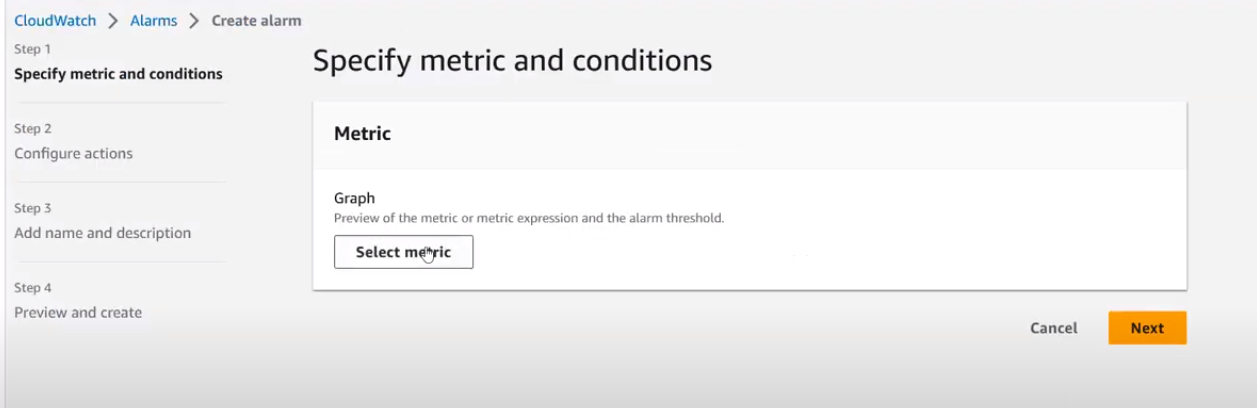
We can share publicly or privately



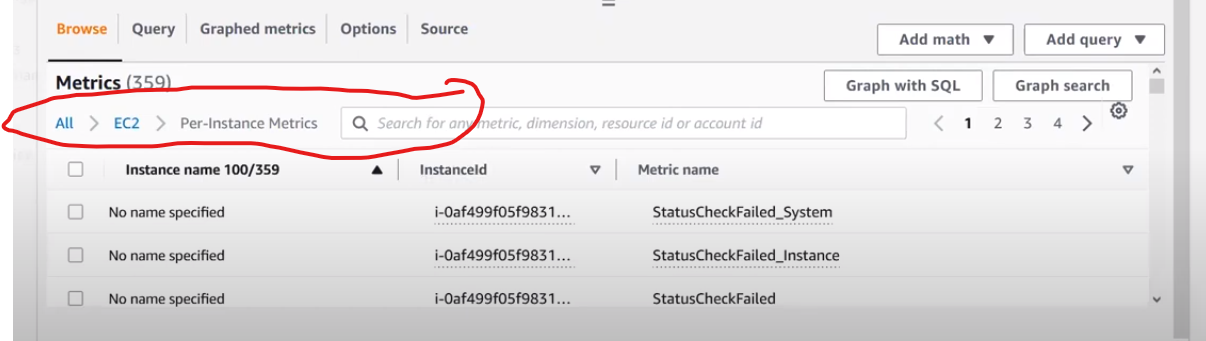
For editing instance id



Create alarm in alarm section

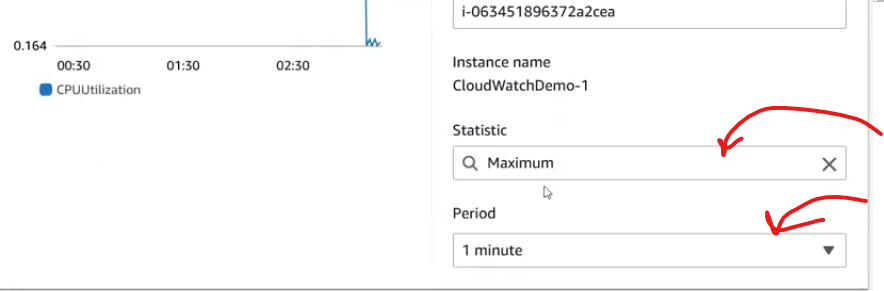


For every alarm you need to select metric

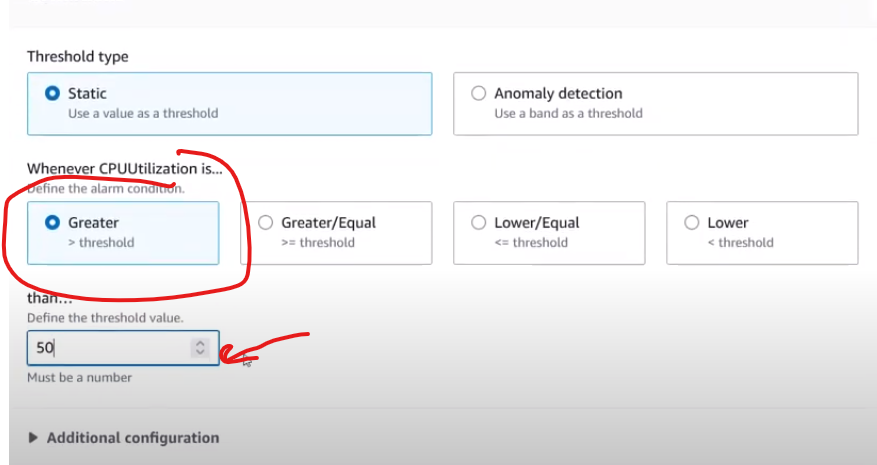


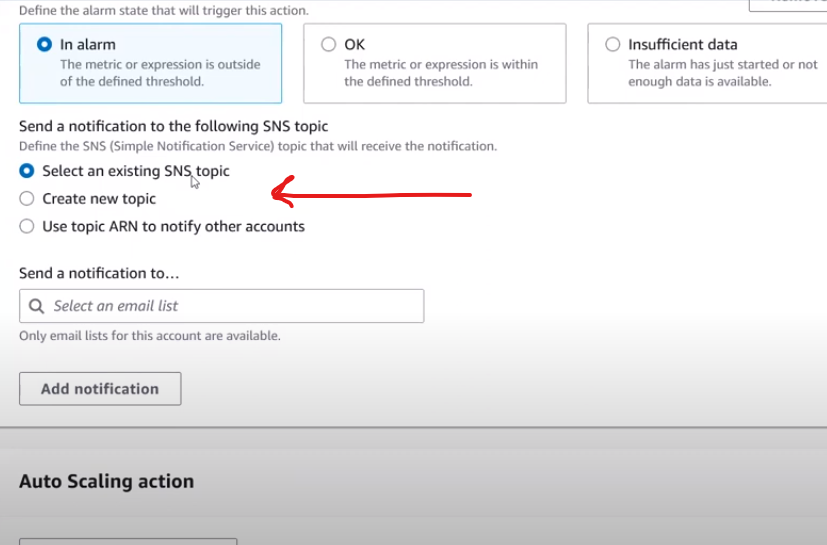
In metrics select -> Ec2-> perinstance metrics-> instance id of your servers

In cpu metrics

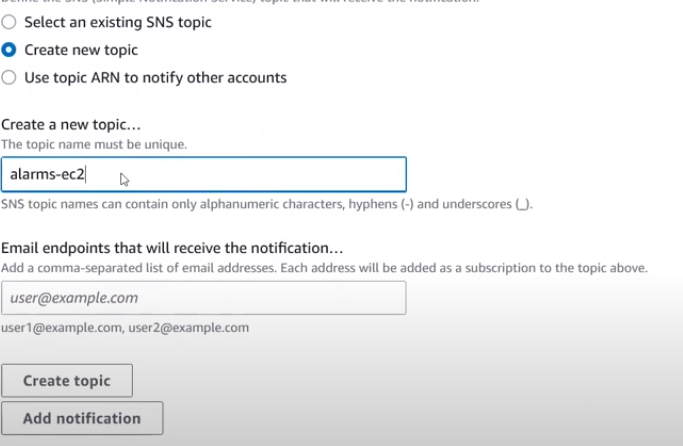


We are keeping a condition with in a 1 min of time max util > 50 % trigger alarm





If you want a notification from service we use simple notification service in aws

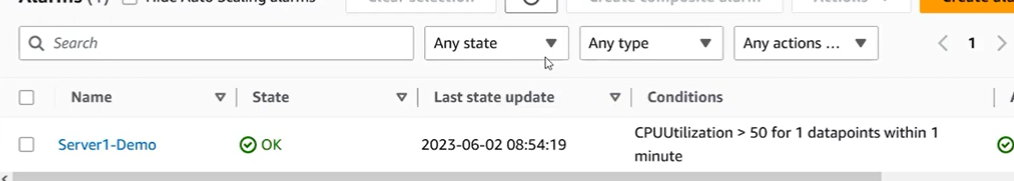


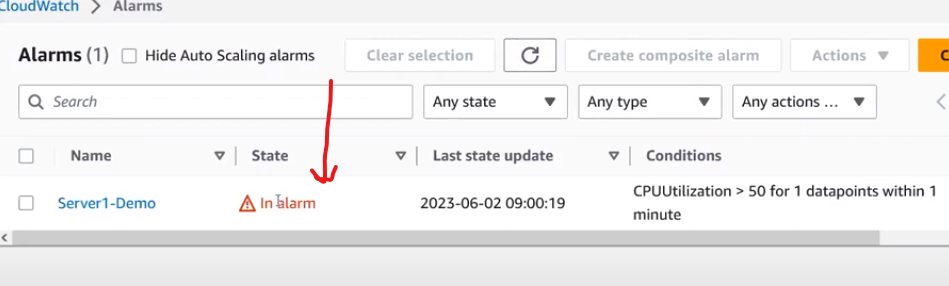
To increase server performance we are using 3 commands

sudo amazon-linux-extras install epel -y

sudo yum install stress -y (yum is a package)

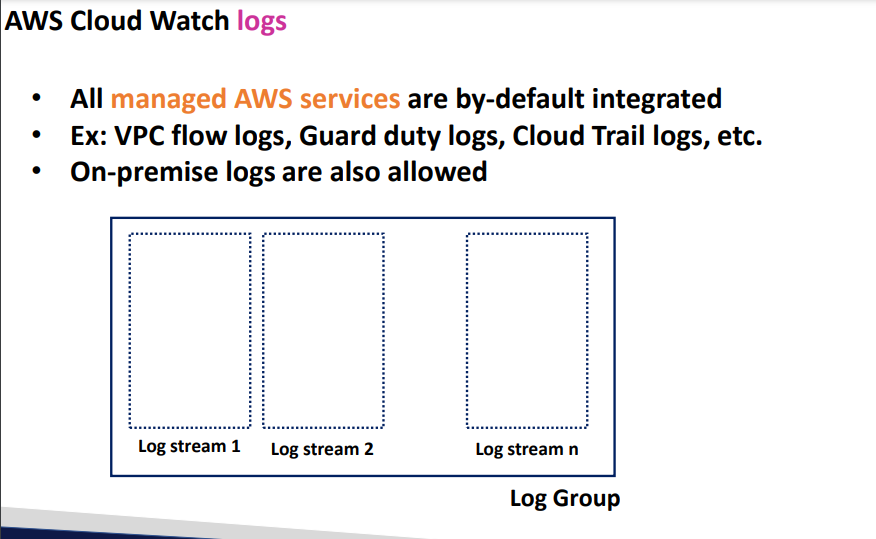
stress -c 1 -t 3600 (1c for 3600 secs to run)





Check your email id for trigger message or mobile no which you gave while creating alarm

After demo delete servers,alarm, dashboards



Log group is application level

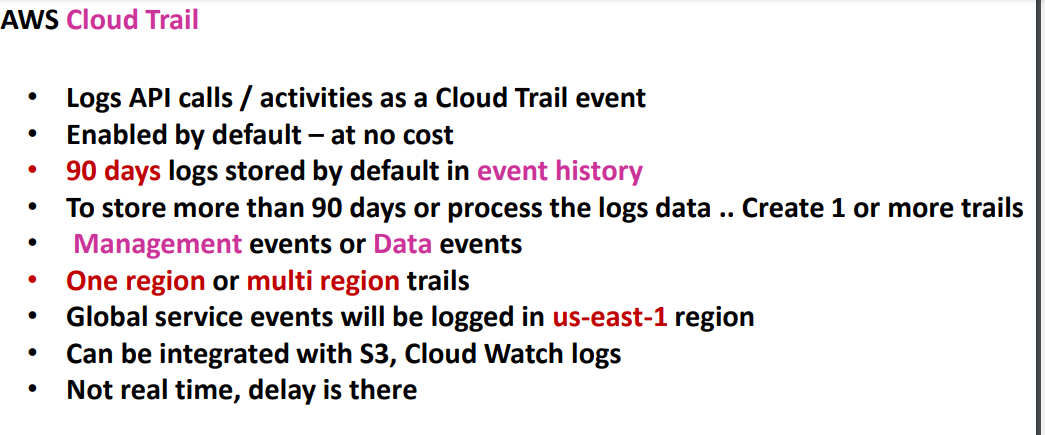
* Log stream is server level
* Like log stream 1, log stream 2 etc etc ………. Log stream n



**Cloud Trail**

1. **Each and every activity is stored in cloud trail**

**For ex : if someone has deleted Ec2 server in cloud trail we can get the info of that particular peron who has deleted the data**

****

**By default aws stores the logs for 90 days for free of cost if u want more than 90 days data u need to create custom logs**

* **Two types of managements are there**

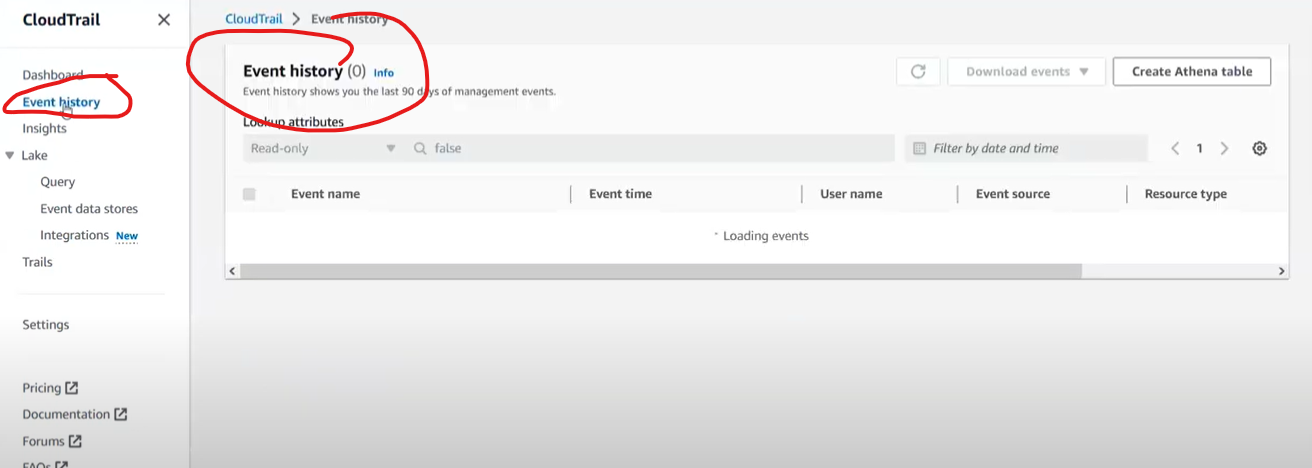
1. **Management events**
2. **Data Events**

* **Management events are the events**

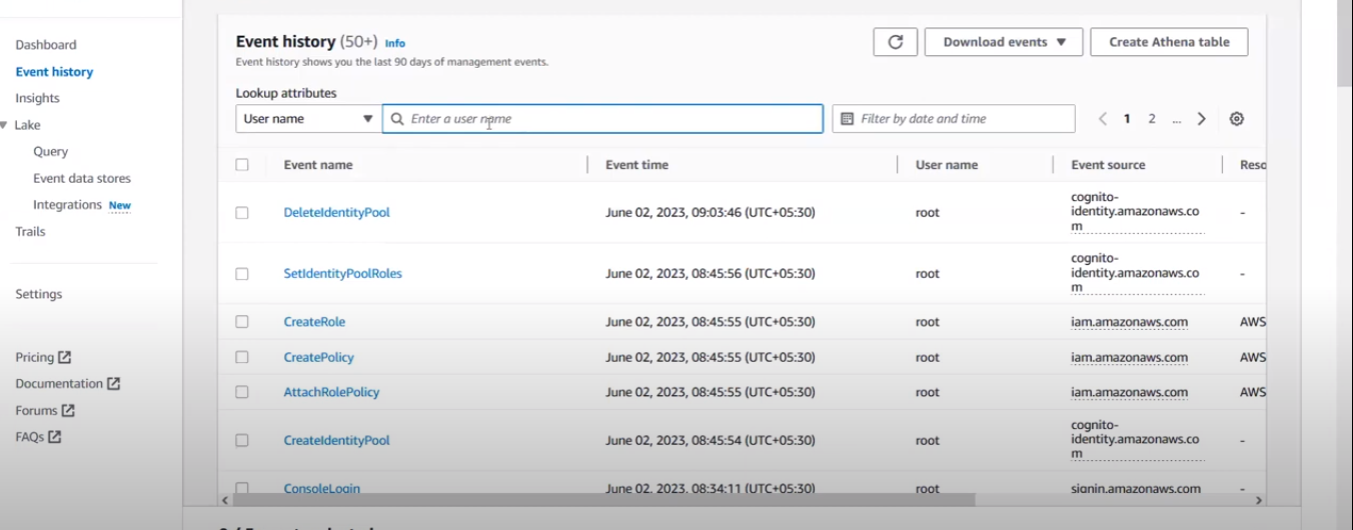
1. **Delete or create or updating the resources comes under management resource**

**Like Ec2, S3,Vpc,subnet**

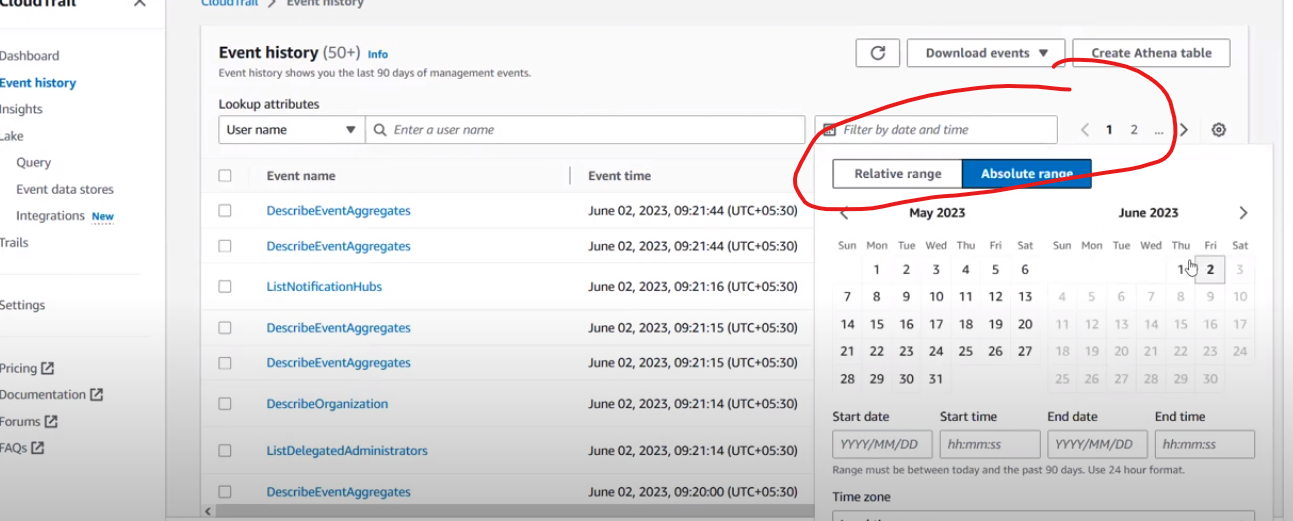
1. **S3 is a resource and inside the s3 buckets files will be stored those are called data**
2. **By default 90 days logs we only get management events logs**
3. **Data events are the events uploading files deleting files in s3 buckets those are called data logs**
4. **In organization level u can create trials how all the account trials will be stored only 1 act i.e for the act which u have created in that act u can able to see**
5. **Global service events will be stored in north virginia region**
6. **I am is a global service so those events will be stored in north virgina region**
7. **Logs can be integrated to s3 or cloud watch logs**
8. **As soon as you create the log there will be 5 mins delay**

****

**In event history you will get to know the history of 90 days which is by default**

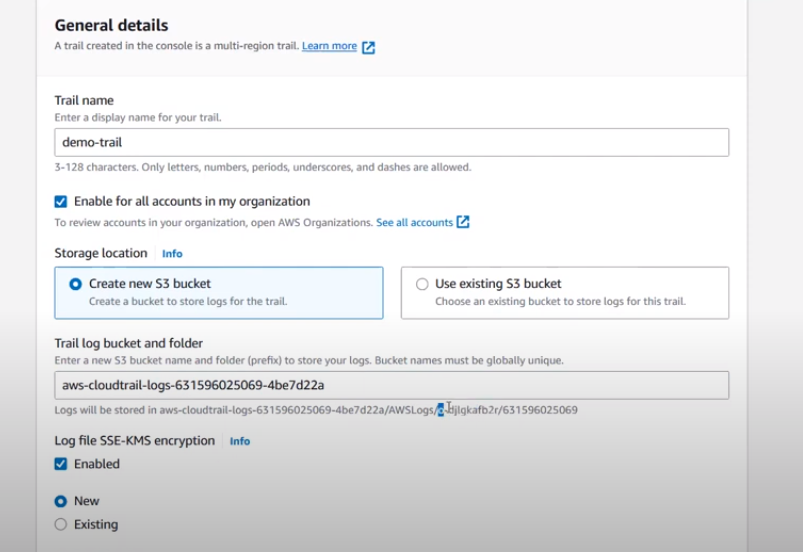
****

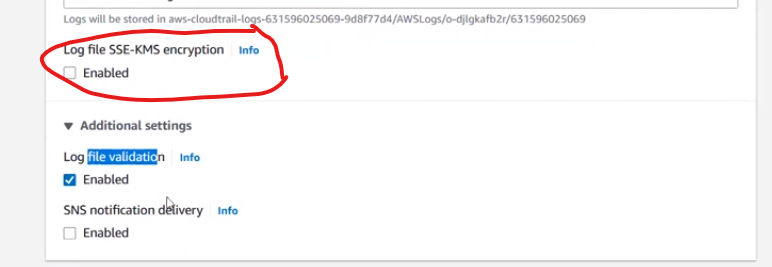
**Even you can filter user name as well**

****

**You can filter time**

**Create custom trial**

****

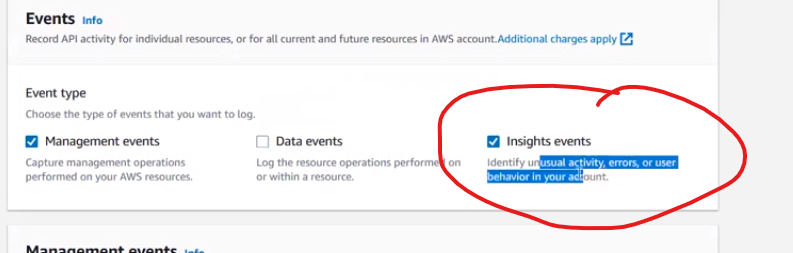
****

**For log file security we enabling log file encryption**

****

**In data events you can collect for multiple files or else custom files for that particular service**

****

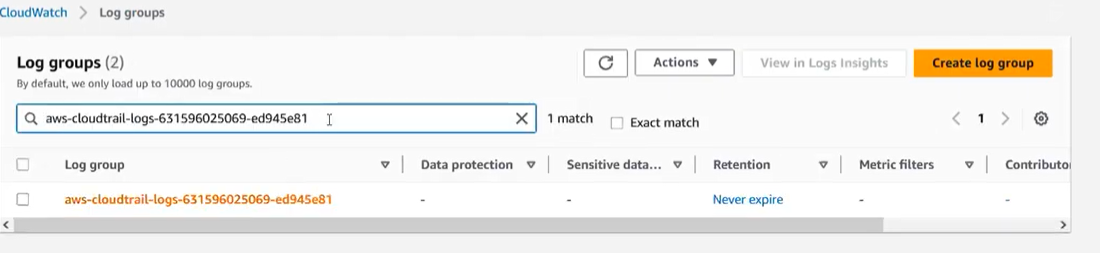
****

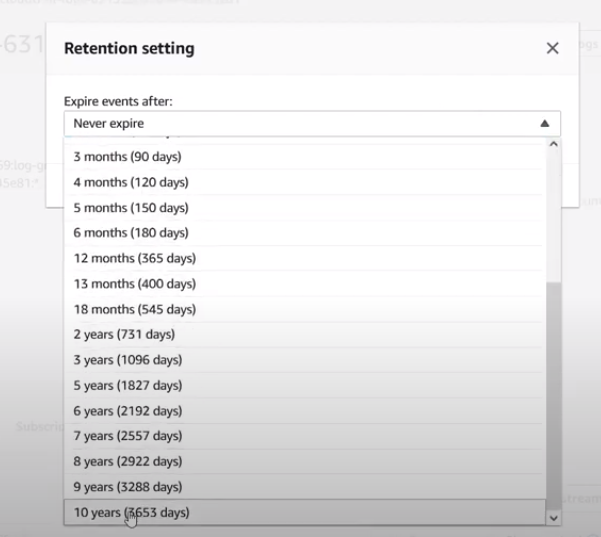
**Unusual activity or errors or user behaviour will be stored in insight events**

**By default aws created integration between cloud watch and cloud trail**

**In cloud trail what ever you have created you can check those logs in s3 buckets**

**And install json gun zip fill in firefox**

****

****

**In logs you can edit when it can expire**

**In realtime for logs visualization**

**They will pull data of logs in to sumologic or splunk etc etc for logs visualization**