**Amazon Web Services (AWS) Cloud Watch**

Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

The CloudWatch home page automatically displays metrics about every AWS service you use. You can additionally create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose.

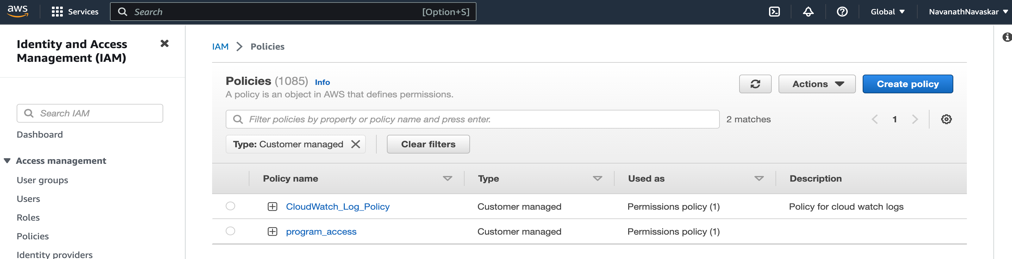
You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached. For example, you can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use that data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money.

1. **Logging data to CloudWatch**

Following are the steps in sending logs from AWS instances (EC2) to CloudWatch:

* Create Policy for IAM Role to allow access to Cloud Watch logs

1. Login to AWS account and click on IAM service.
2. Under Policies -> Click on “Create Policy”



1. Click on JSON tab and copy paste below data

*{*

*"Version": "2012-10-17",*

*"Statement": [*

*{*

*"Sid": "Statement1",*

*"Effect": "Allow",*

*"Action": [*

*"logs:CreateLogGroup",*

*"logs:CreateLogStream",*

*"logs:PutLogEvents",*

*"logs:DescribeLogStreams"*

*],*

*"Resource": [*

*"arn:aws:logs:\*:\*:\*"*

*]*

*}*

*]*

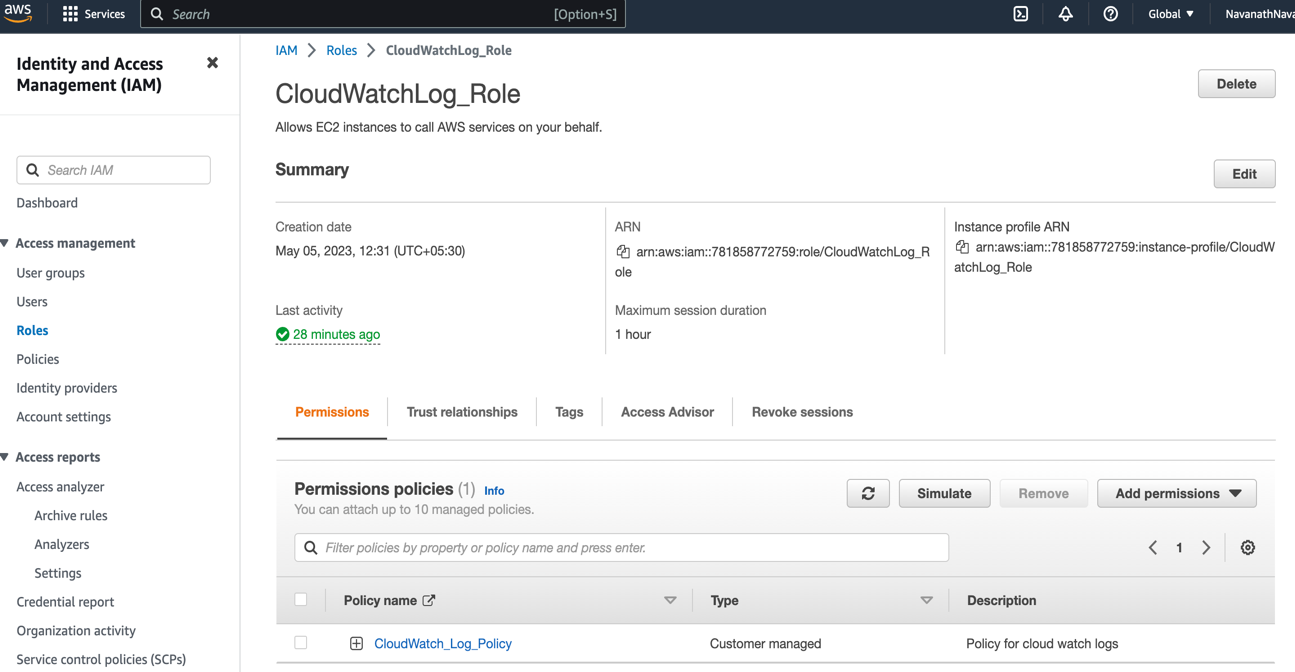
*}*

1. Click on “Next”
2. Add Policy Name, Description and Tags if required.
3. Click on Create policy. See CloudWatch\_Log\_Policy below

A screenshot of a computer

Description automatically generated with medium confidence

* Create IAM Role with above policy for EC2 instance. See CloudWatchLog\_Role below



* Create EC2 instance and assign IAM Role “CloudWatchLog\_Role” to EC2 instance
* SSH to this EC2 instance using public key with ec2-user and public key

1. Install awslogs -> CloudWatch agent for linux using below command

*yum install awslogs -y*

1. We need to now configure cloud watch client. Update *“/etc/awslogs/awscli.conf”* file with correct region name
2. Now update *“/etc/awslogs/awslogs.conf”* file like given below:

*[general]*

*state\_file = /var/lib/awslogs/agent-state*

*[application\_logs]*

*region = us-east-1*

*datetime\_format = %b %d %H:%M:%S*

*file = /var/log/application.log*

*buffer\_duration = 5000*

*log\_stream\_name = {instance\_id}*

*initial\_position = start\_of\_file*

*log\_group\_name = my\_app\_logs*

1. Here we are using “/var/log/application.log” file. CloudWatch agent will read logs from this file and send it to Cloud Watch under Log Group “my\_app\_logs”
2. Start the awslogsd service using *“systemctl start awslogsd.service”*
3. Debugging info can be found at <https://repost.aws/knowledge-center/push-log-data-cloudwatch-awslogs>
4. Now write message to application.log file. Wait for few seconds, you can see message in CloudWatch under Log Group.
5. **Setting Alarms**

* Create Log Metric Filter
* Add Filter pattern “ERROR”
* Click on Assign Metric
* Create Filter and exit
* Now Add Alarm for Metric
* Give details and add Action Details
* Now when ERROR string is found in logs, it will generate Email notification to given user