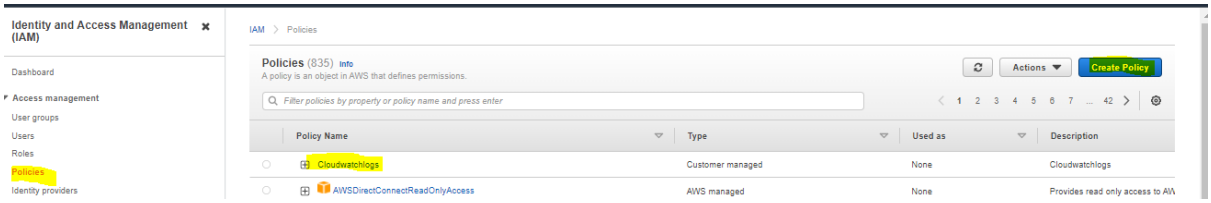
Cloud Watch Logs

Step:1

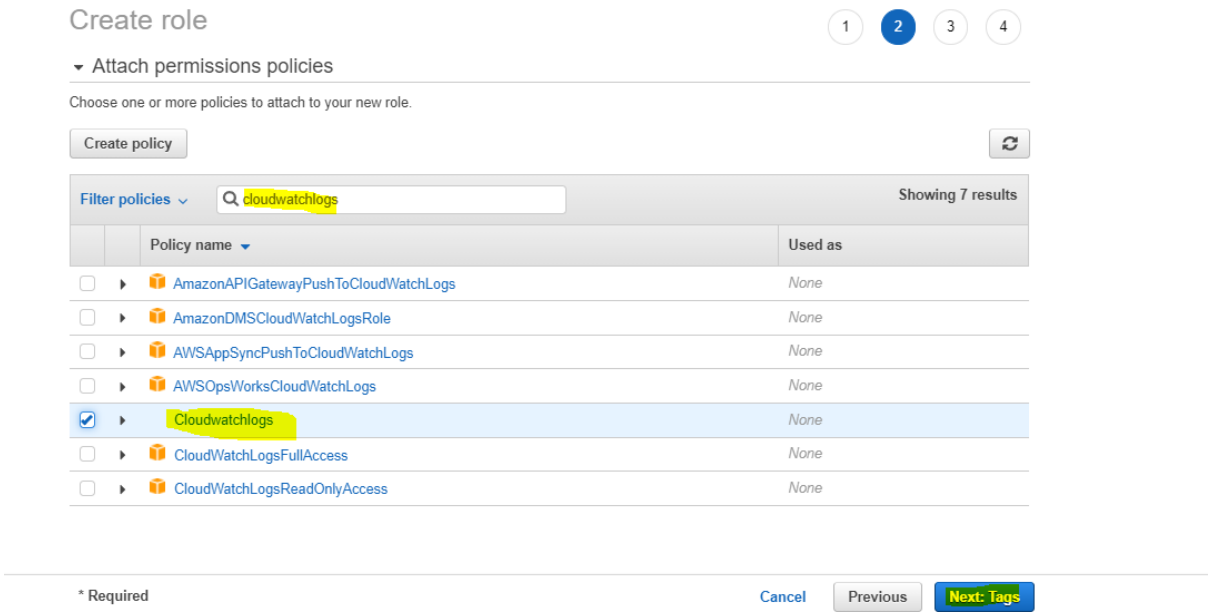
Create a custom policy using JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
    ],
      "Resource": [
        "*"
    ]
  }
 ]
}
```



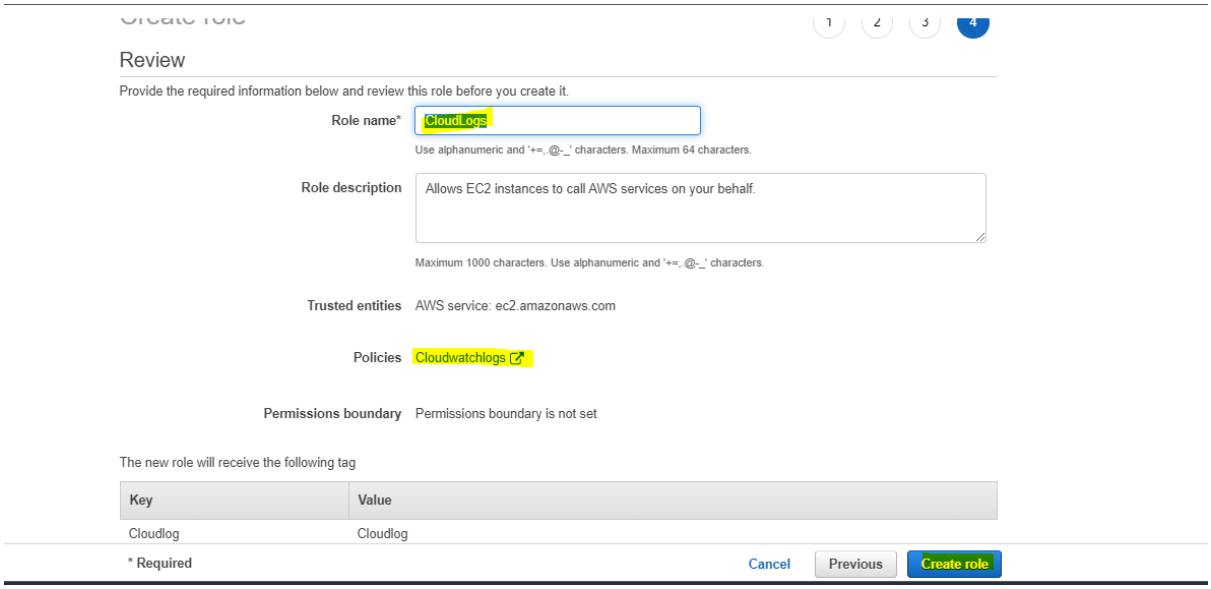
Step:2

Add that custom policy to the role



Step:3

Review the role and create it



Step:4

Create a webserver allow port 80 and attach the IAM role to the particular server.

#!/bin/bash

sudo su

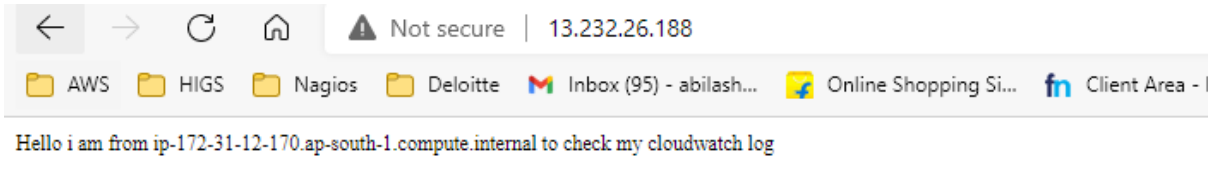
yum update -y

yum install httpd -y #apache

systemctl start httpd

systemctl enable httpd #server restart

echo "Hello i am from $(hostname -f) to check my cloudwatch log" > /var/www/html/index.html

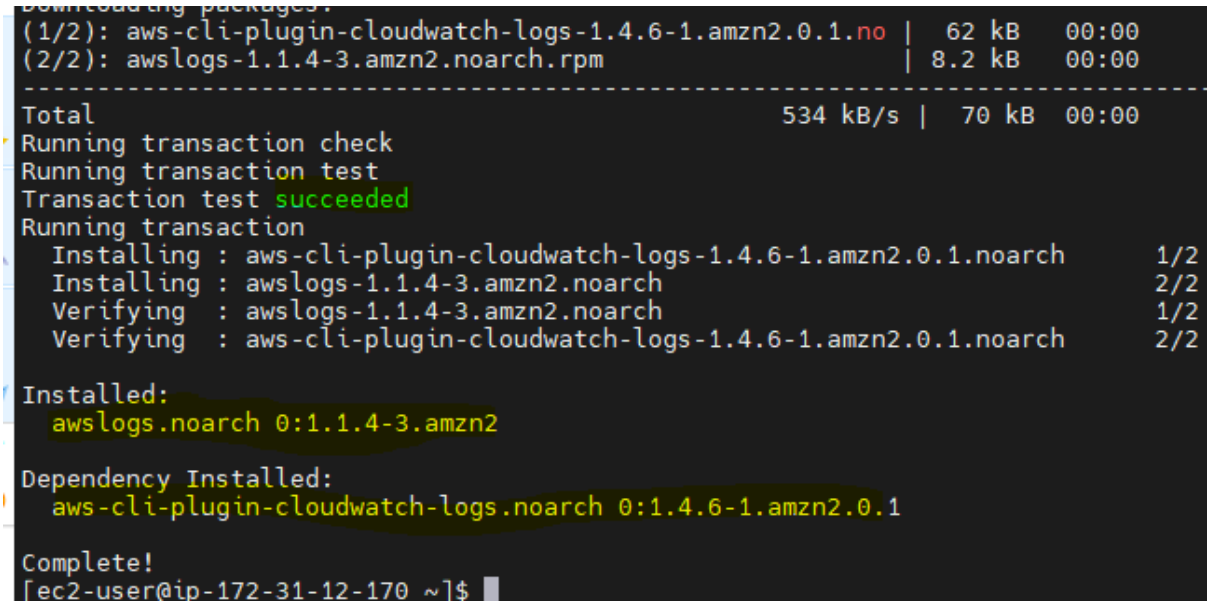


Step:5

Login to the server update and Install the awslogs package.

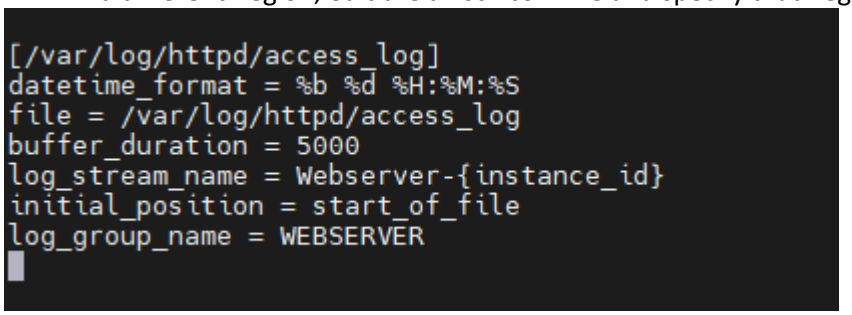
sudo yum update -y

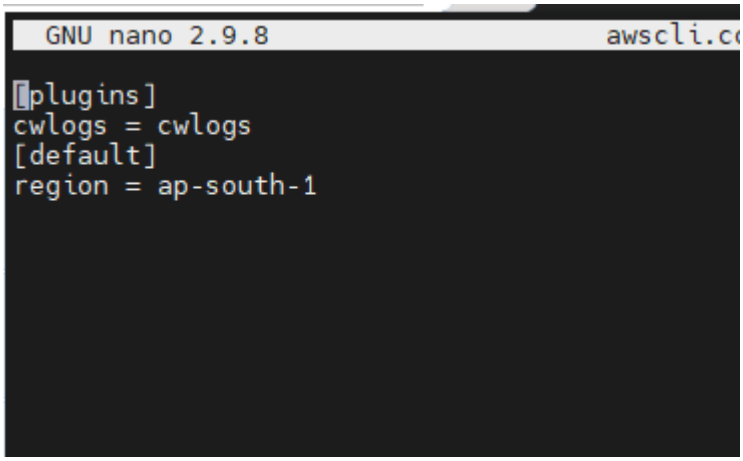
sudo yum install -y awslogs



Step:6

- Edit the /etc/awslogs/awslogs.conf file to configure the logs to track.
- By default, the /etc/awslogs/awscli.conf points to the us-east-1 Region. To push your logs to a different Region, edit the awscli.conf file and specify that Region.





Step:7

If you are running Amazon Linux 2, start the awslogs service and enable it on system boot.

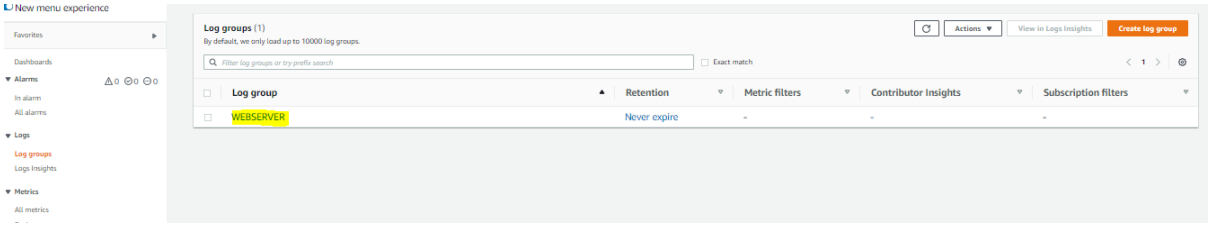
sudo systemctl start awslogsd

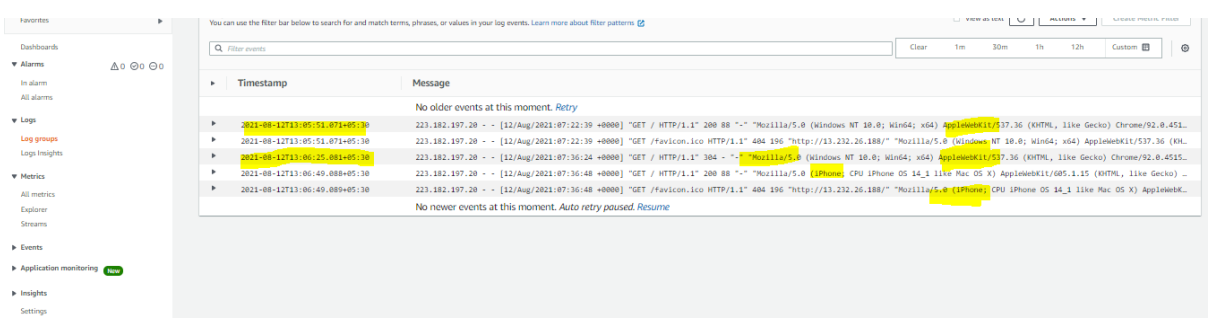
sudo systemctl enable awslogsd.service

```
[ec2-user@ip-172-31-12-170 awslogs]$ sudo systemctl start awslogsd
[ec2-user@ip-172-31-12-170 awslogs]$ sudo systemctl enable awslogsd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/awslogsd.servic
e to /usr/lib/systemd/system/awslogsd.service.
```

Step:8

Access the site and check the logs in the cloud watch logs section you can able to see the logs





IT WORKS 😊