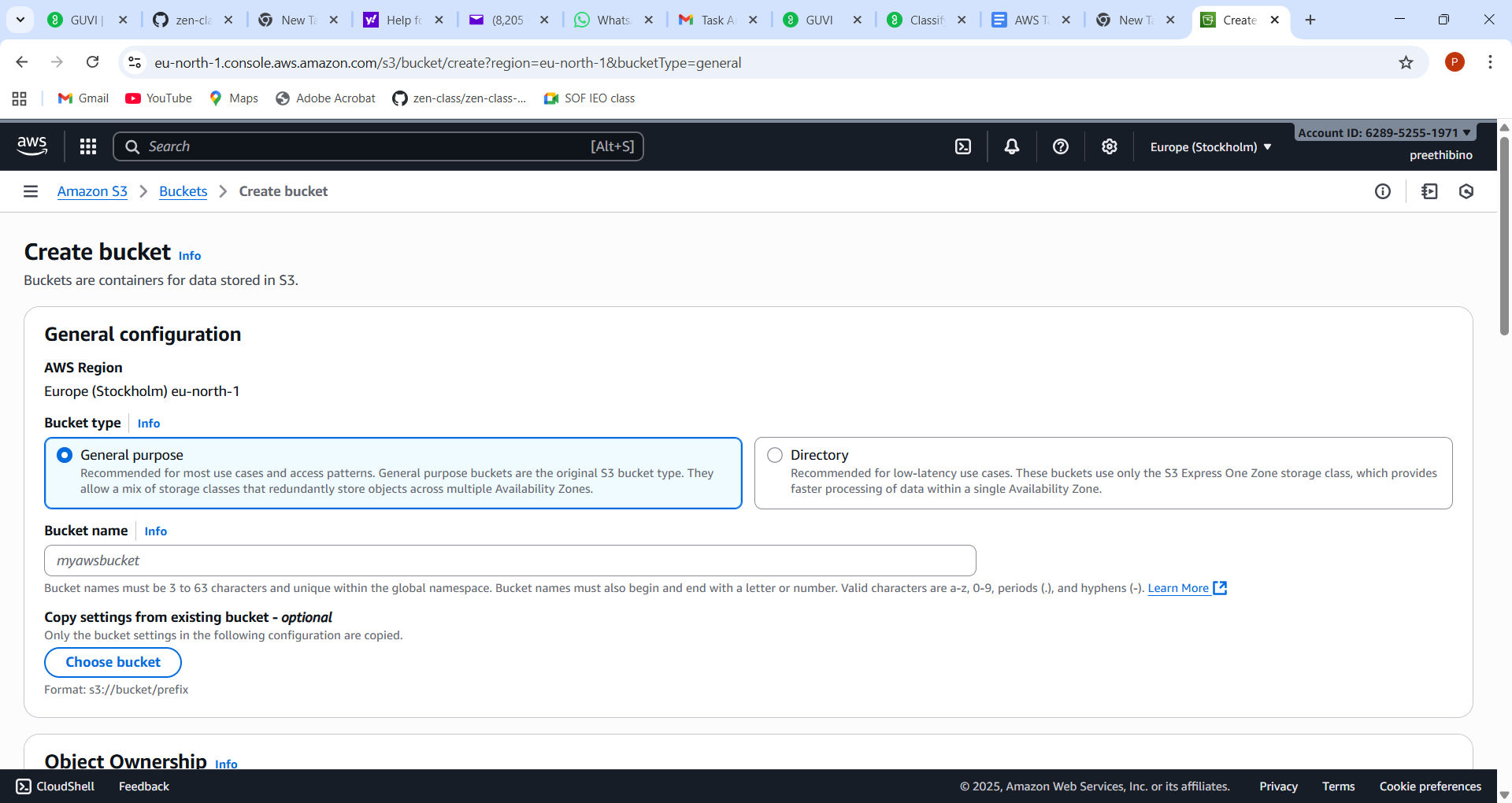
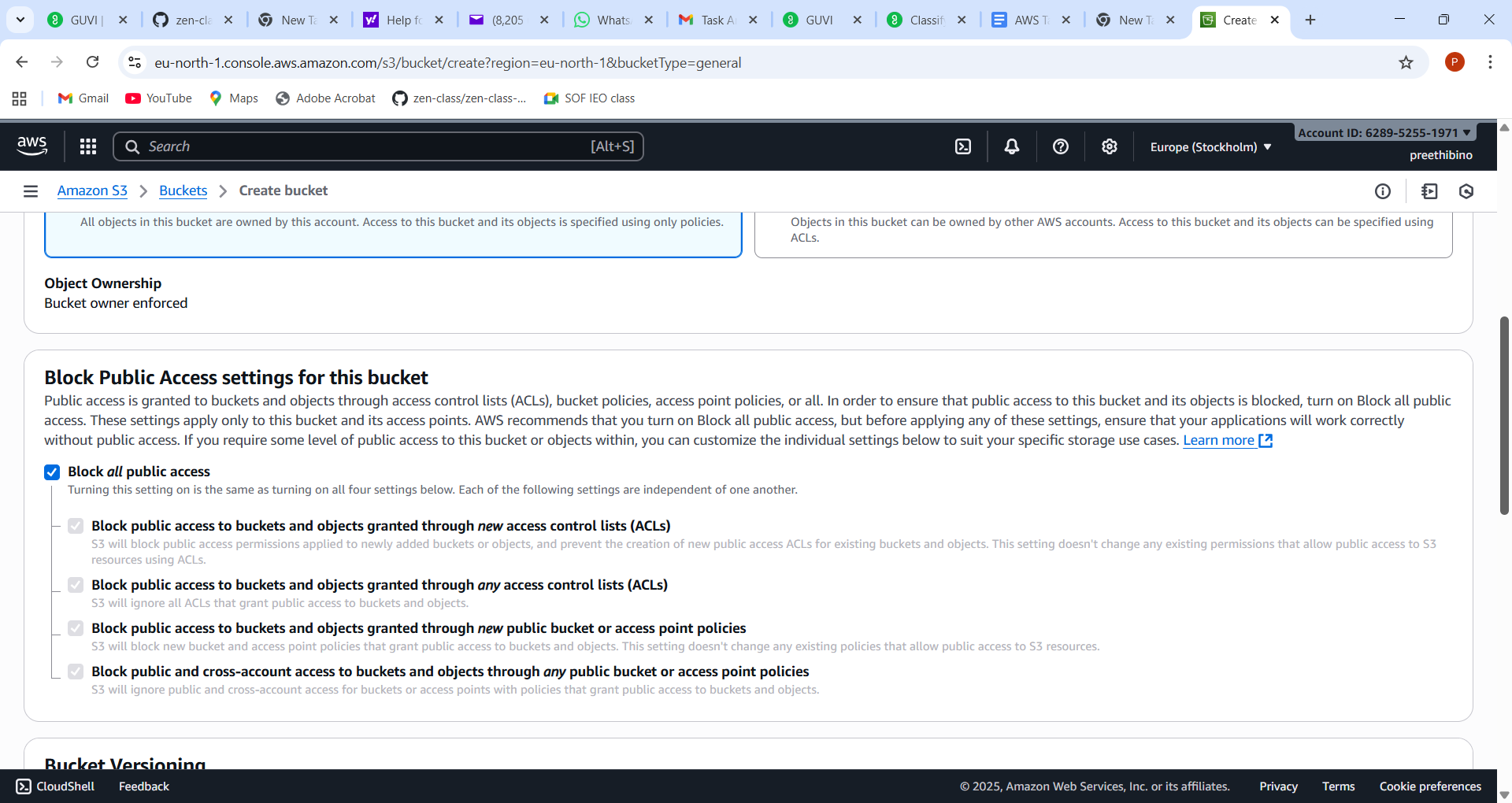
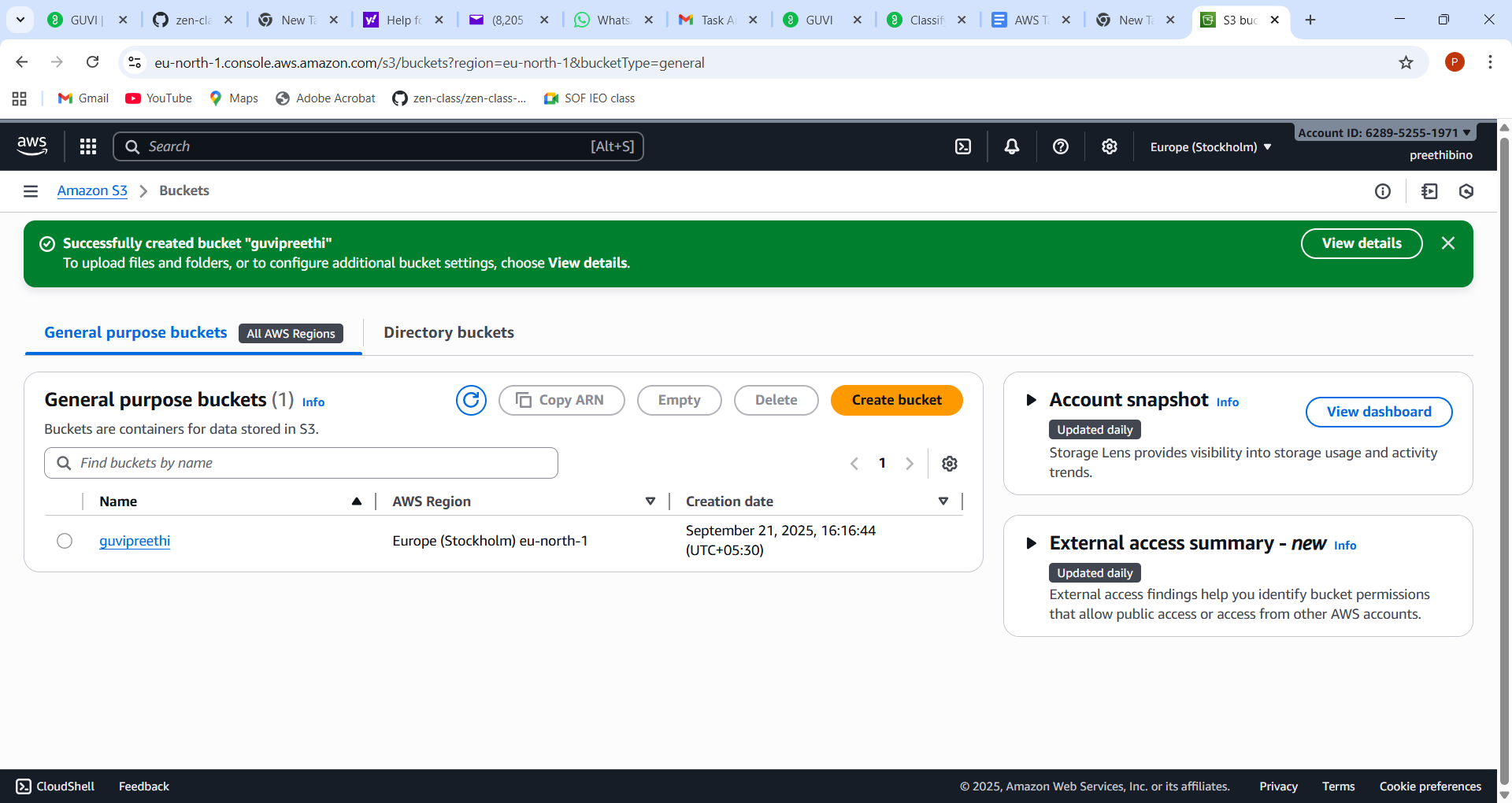
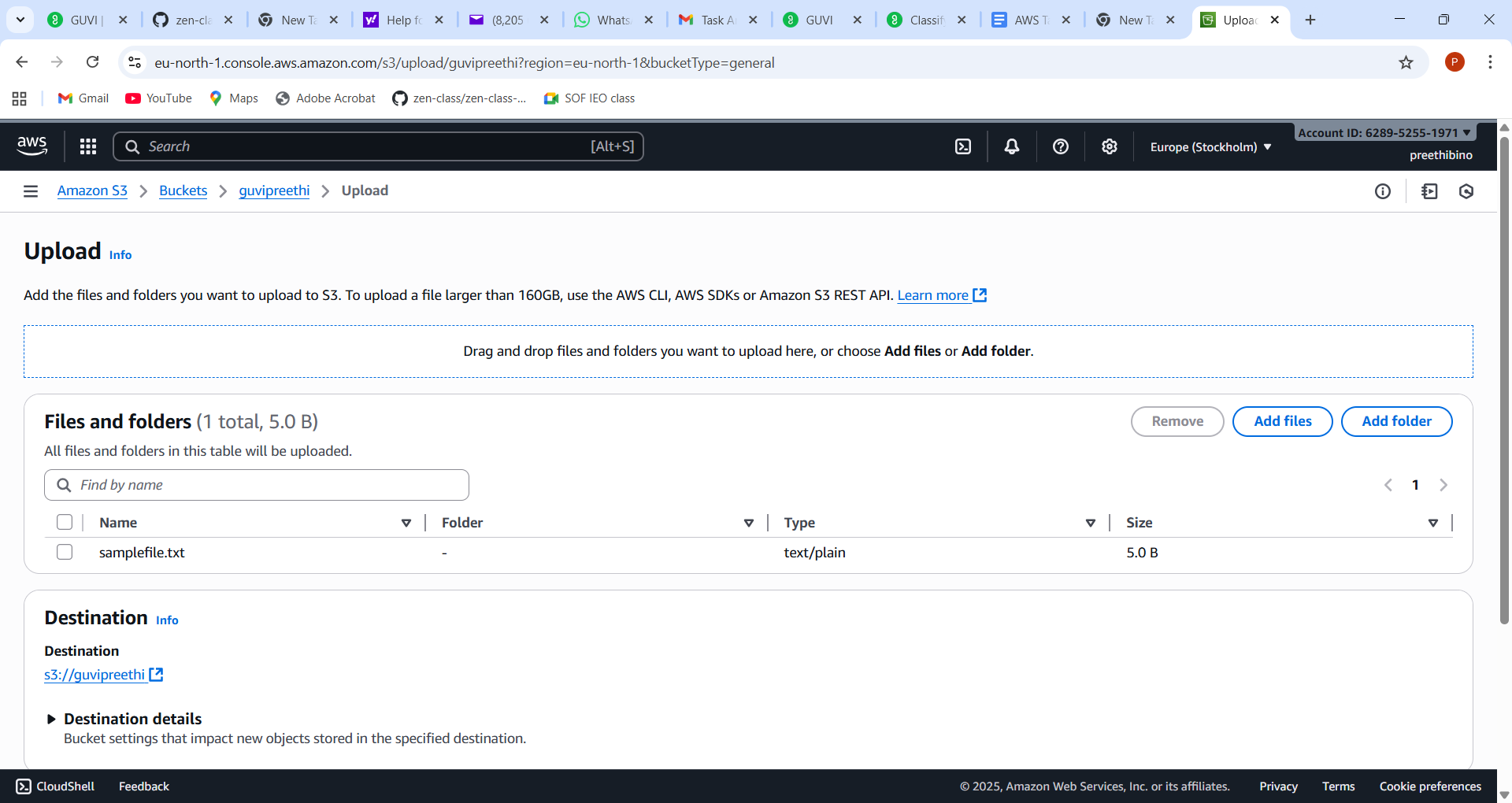
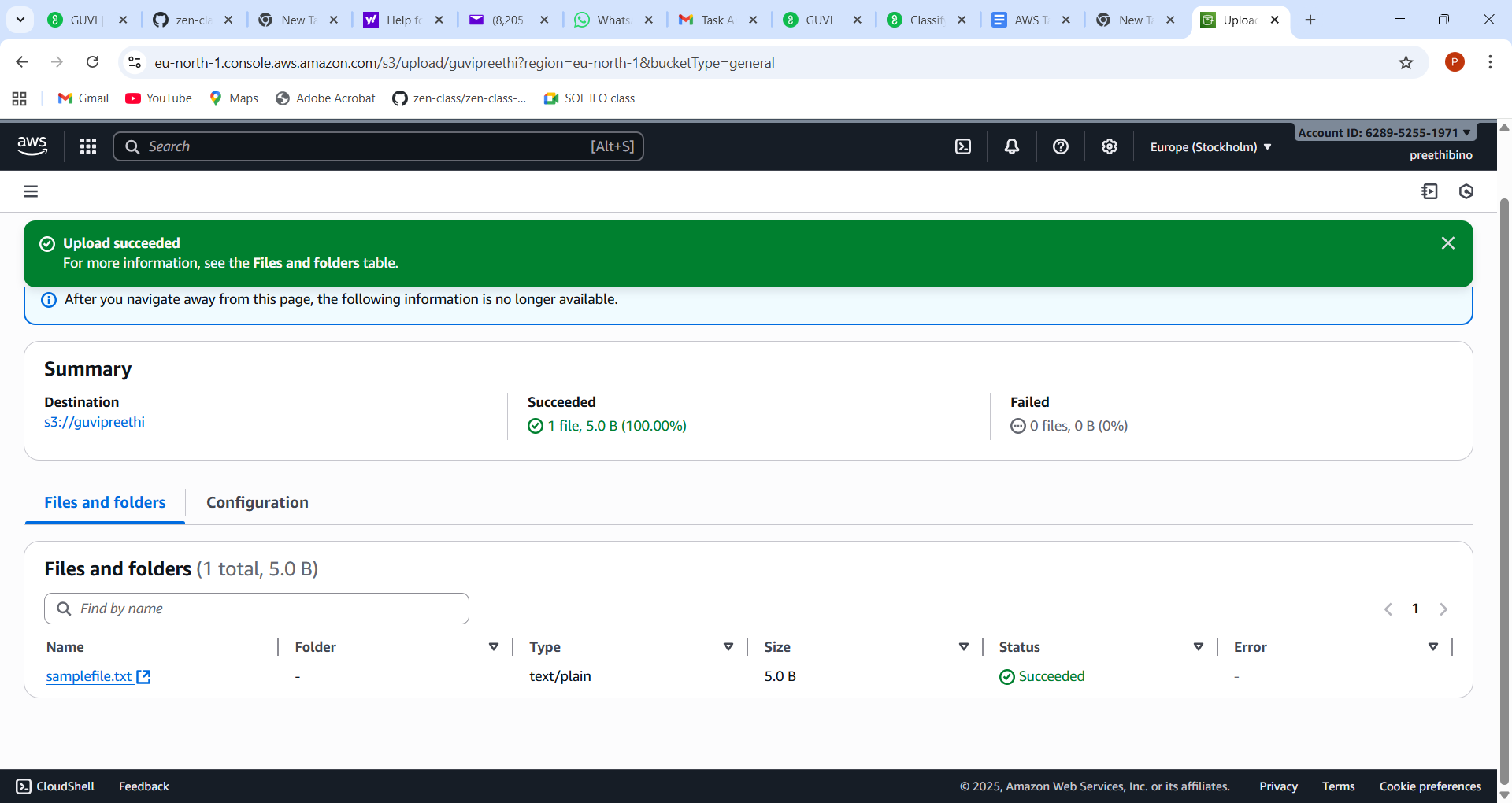
Create a S3 bucket, with no public access and upload files to the bucket & view the logs using cloudwatch for the uploaded files.

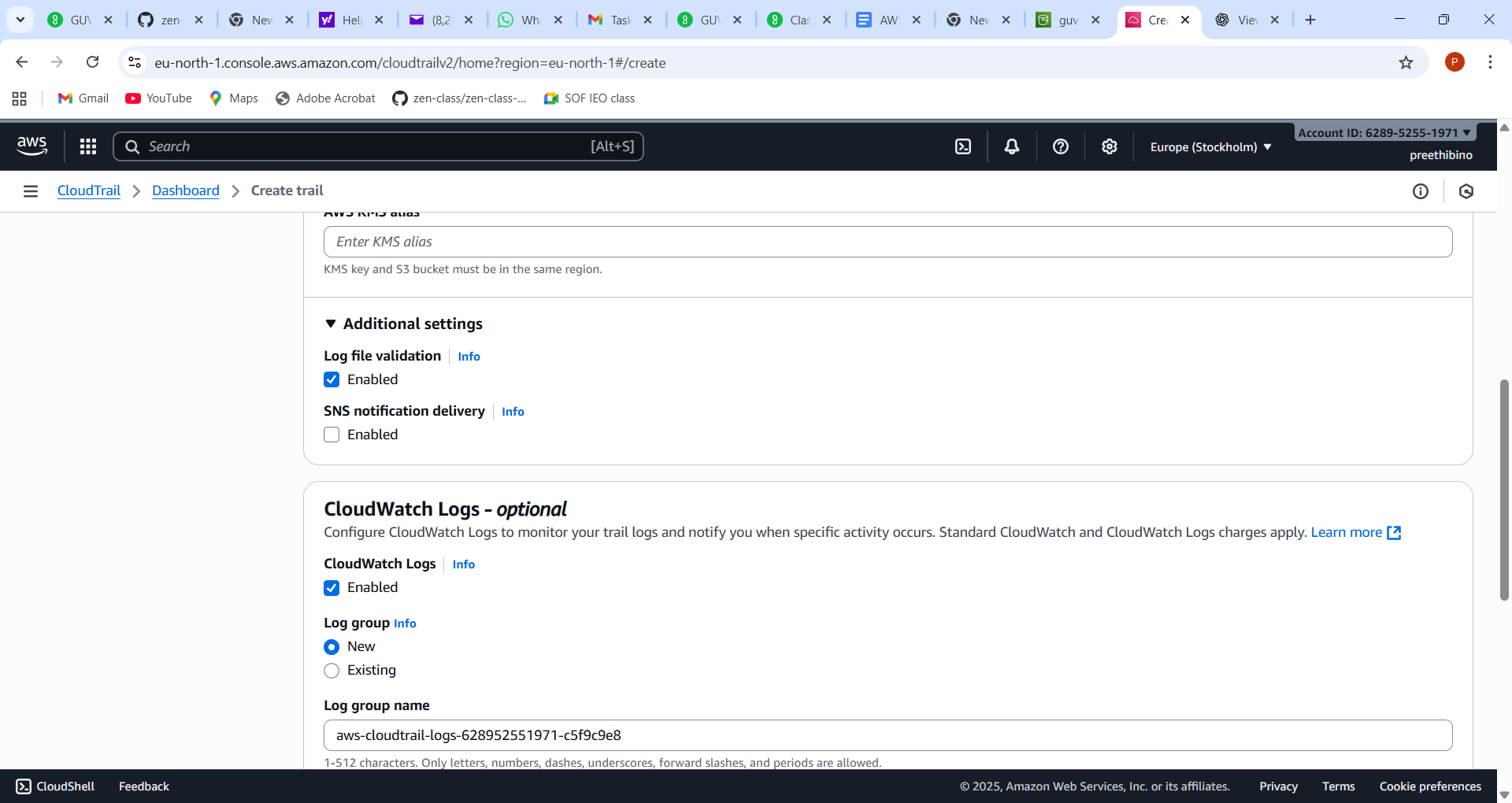


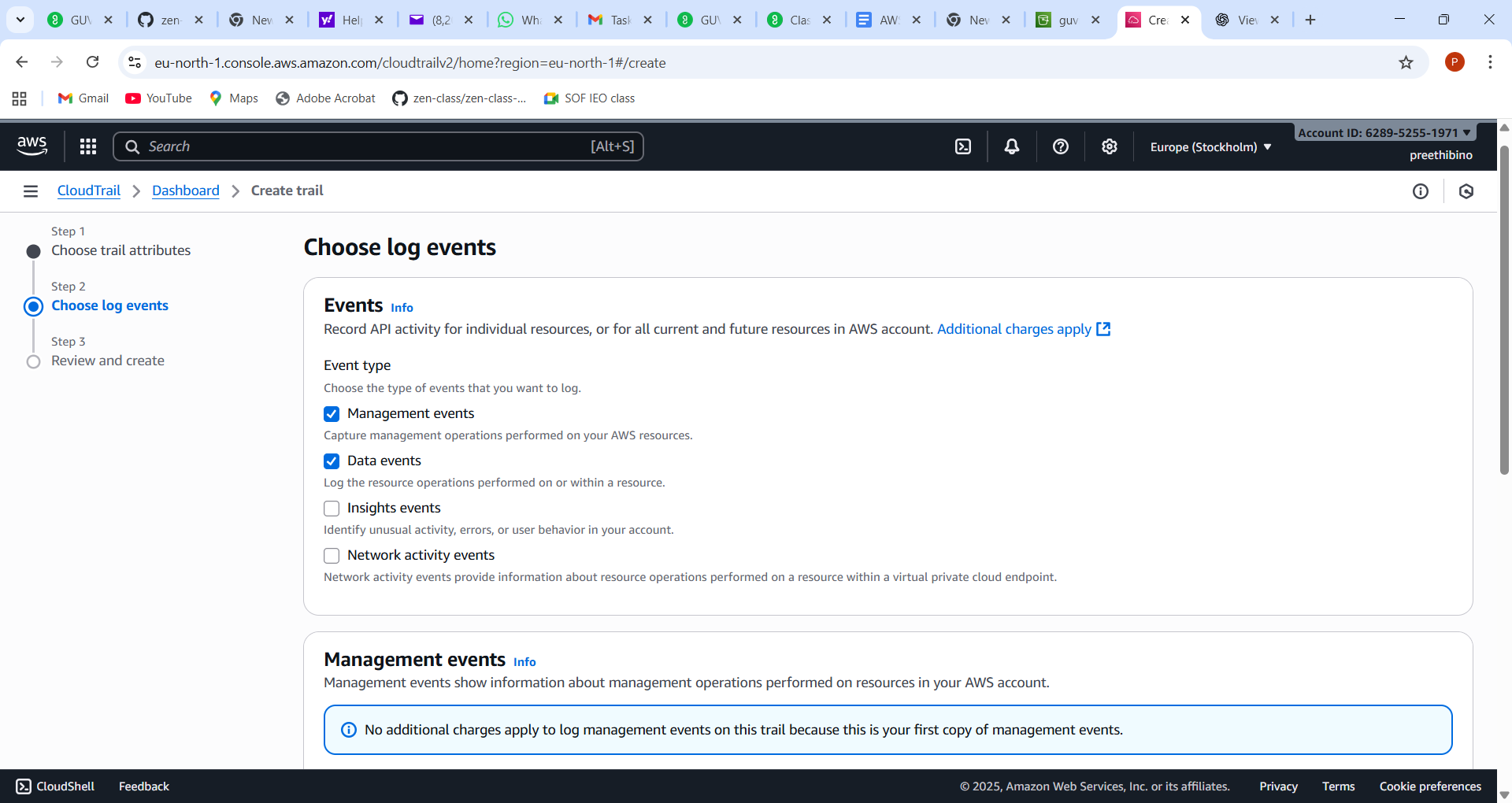


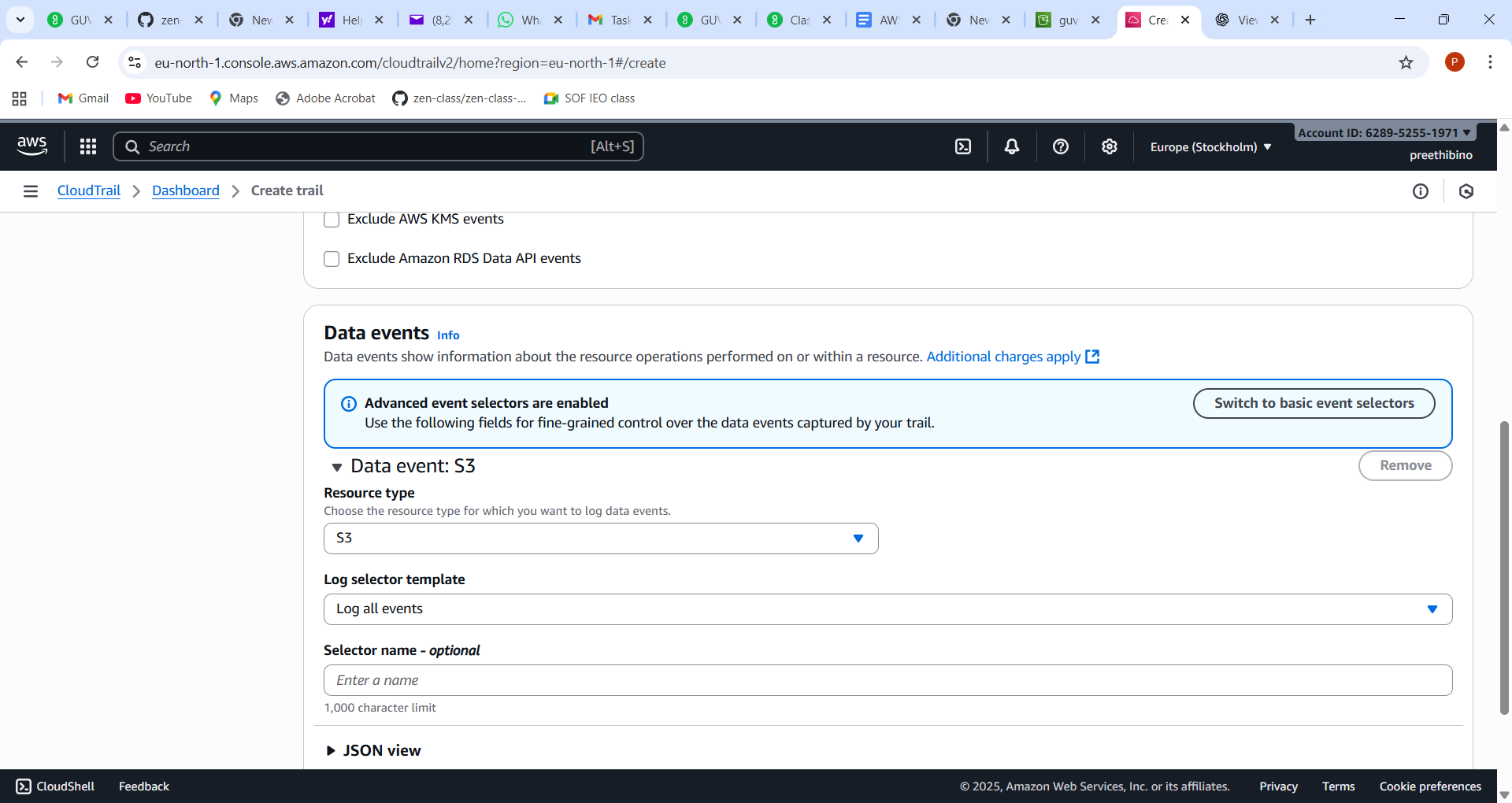


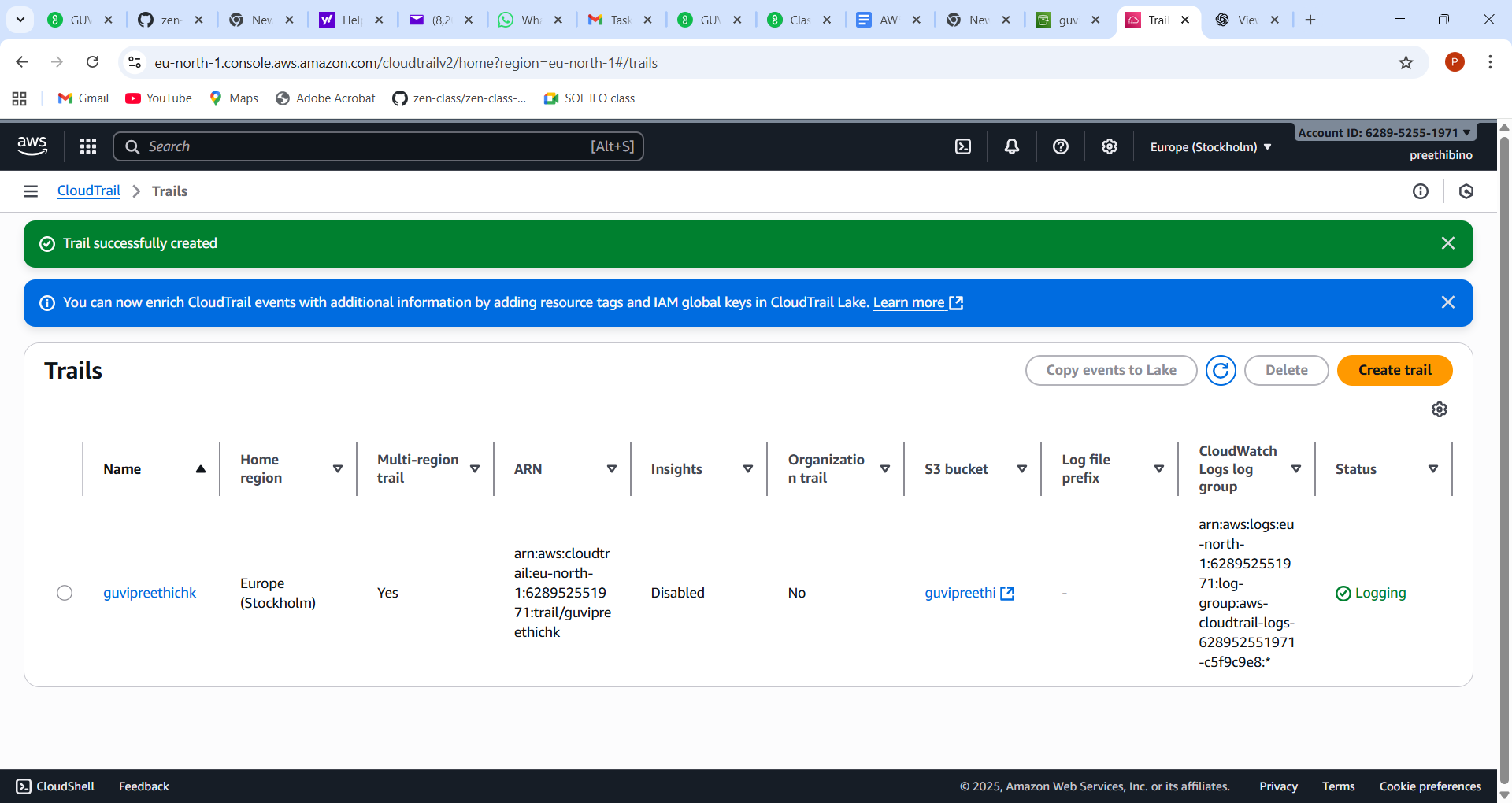


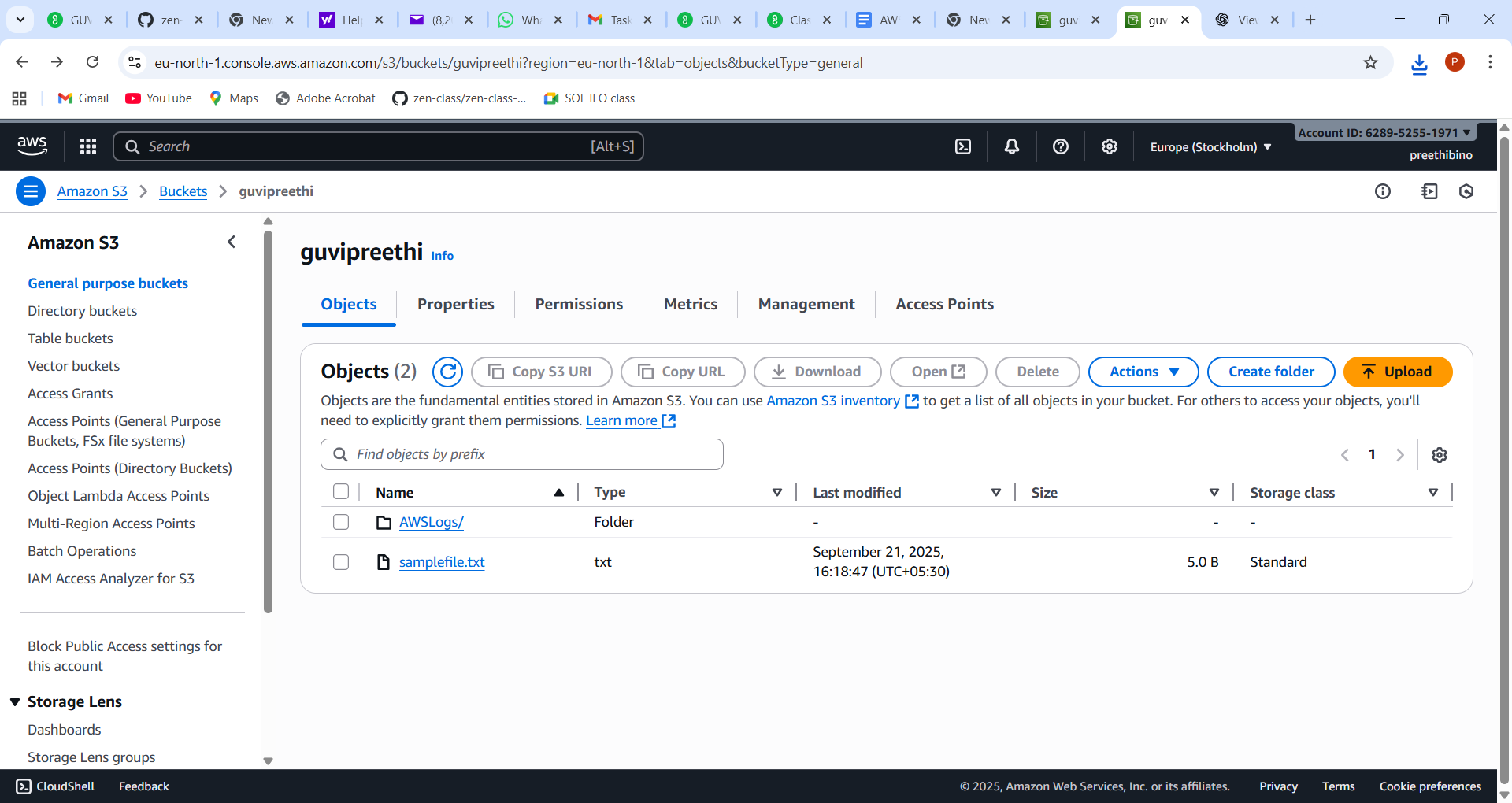


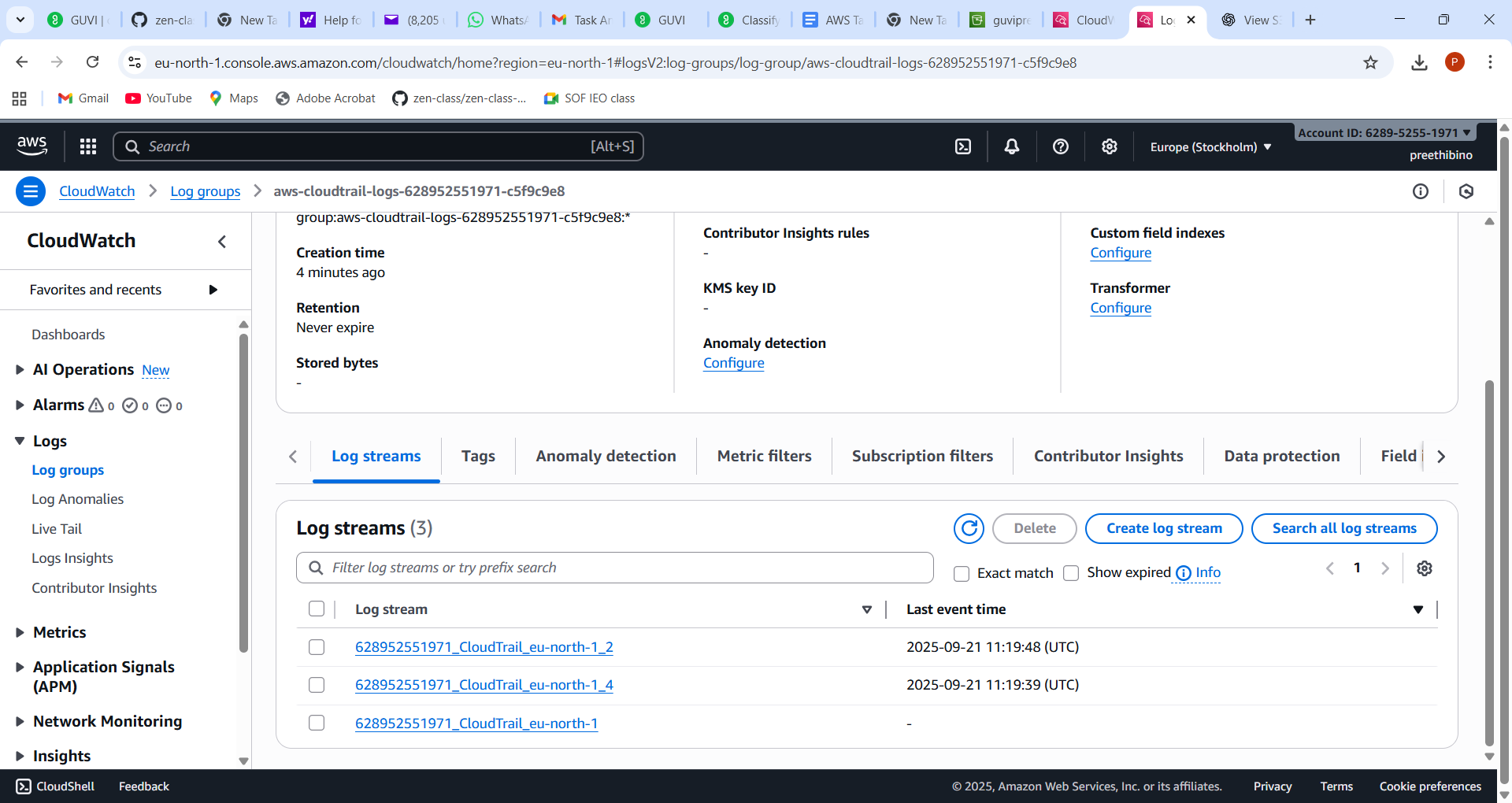






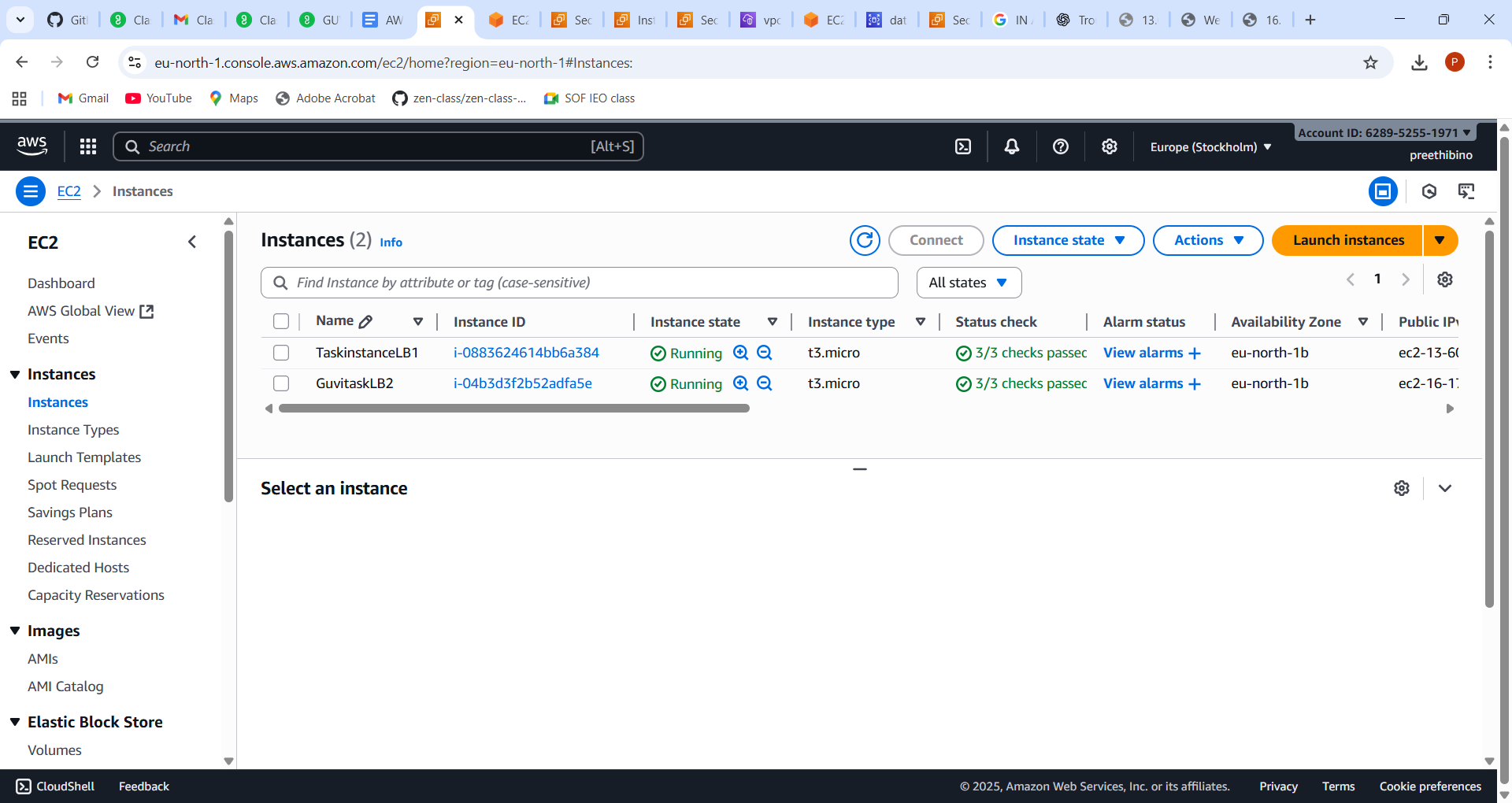




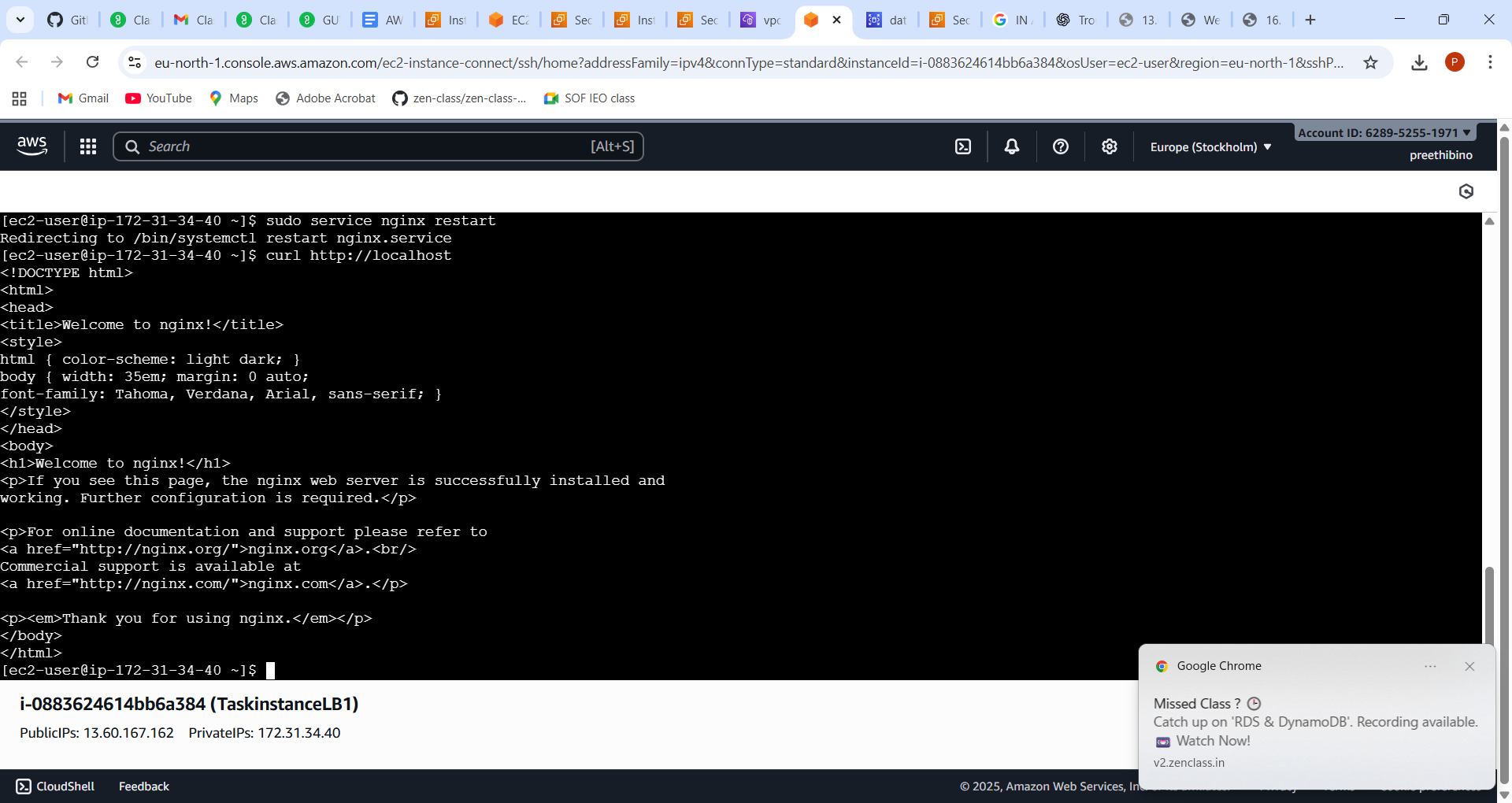


Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

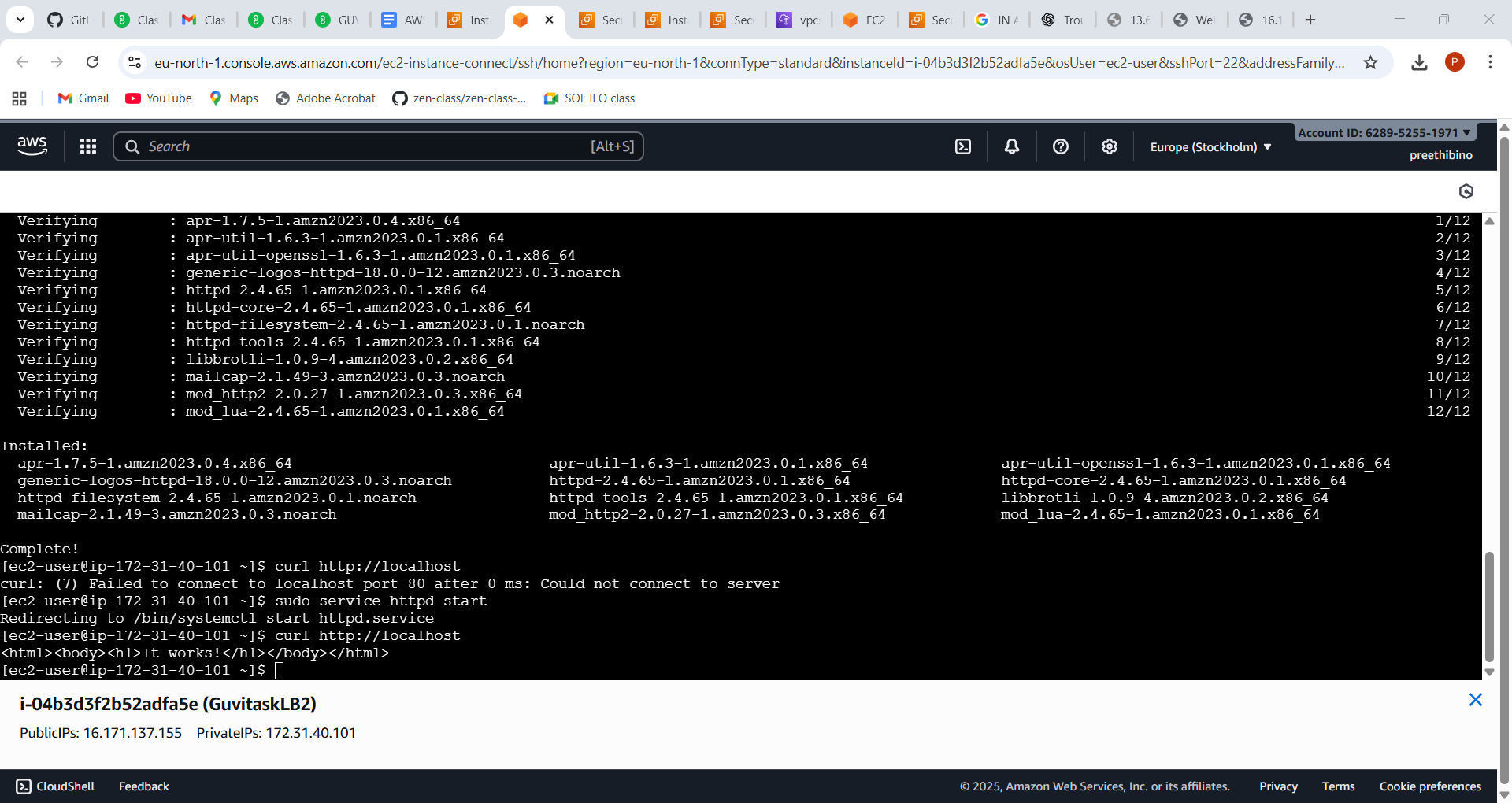
Launch two instance



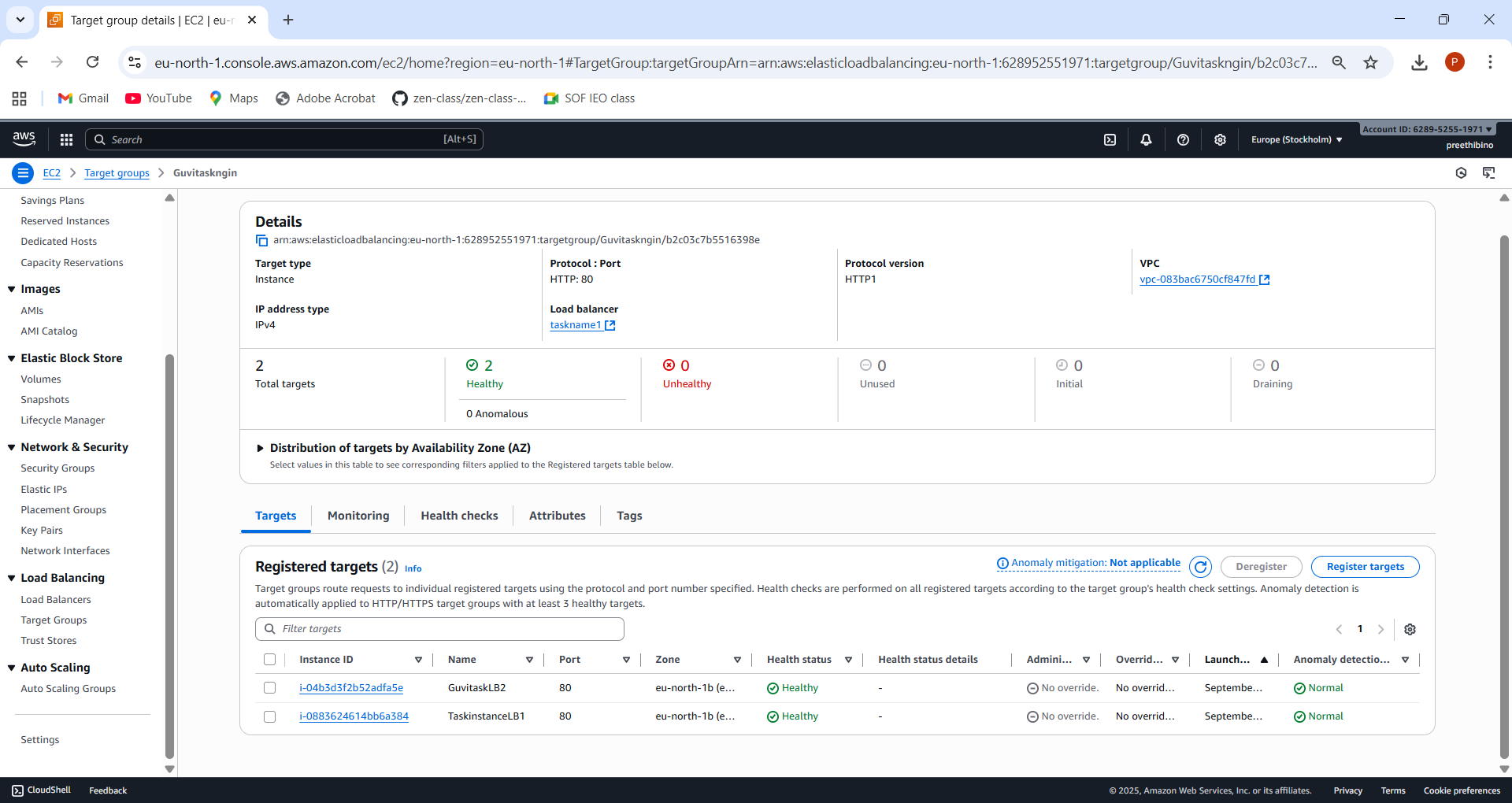
In one instance – launch nginx



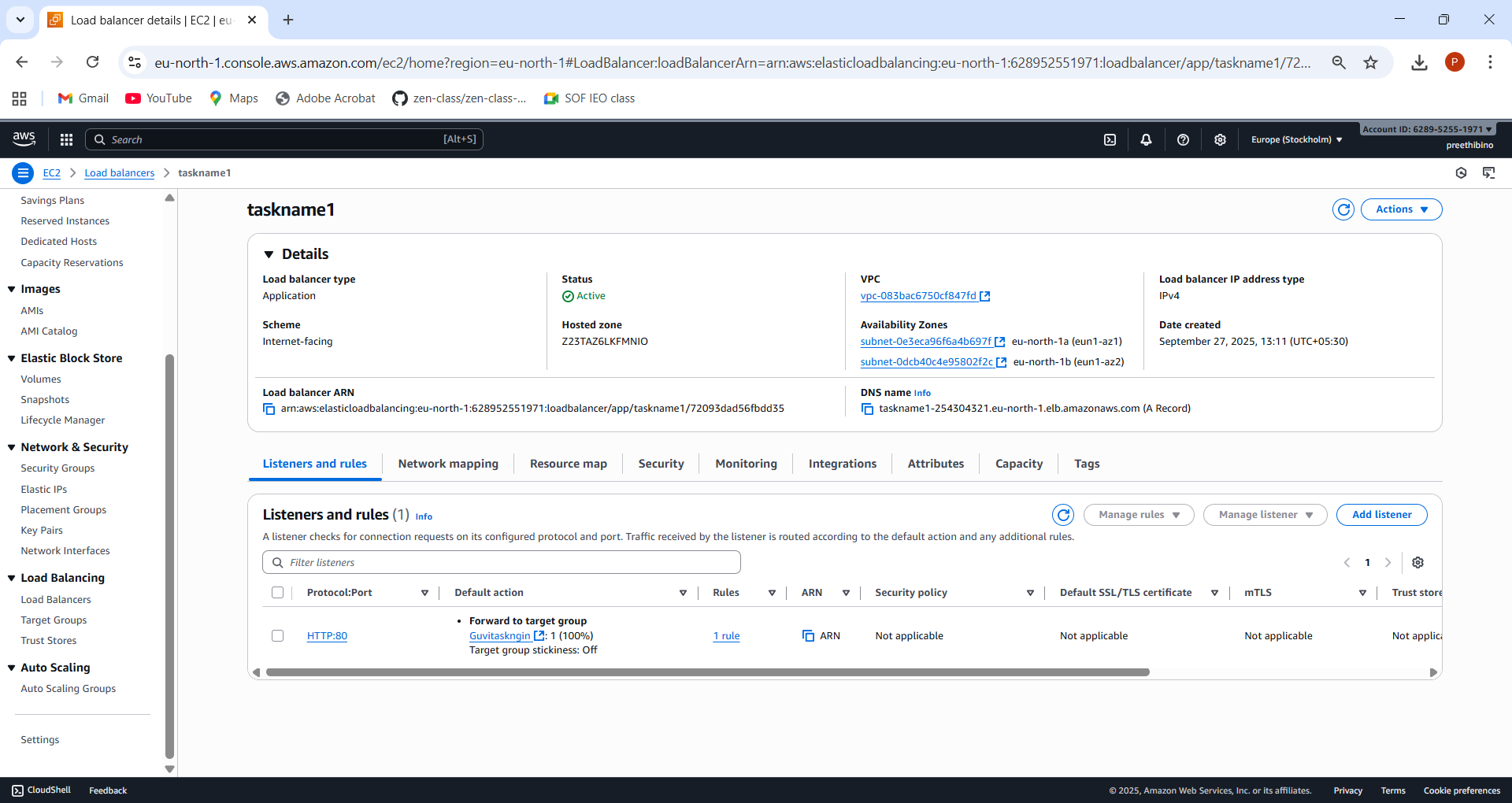
In another instance launch httpd



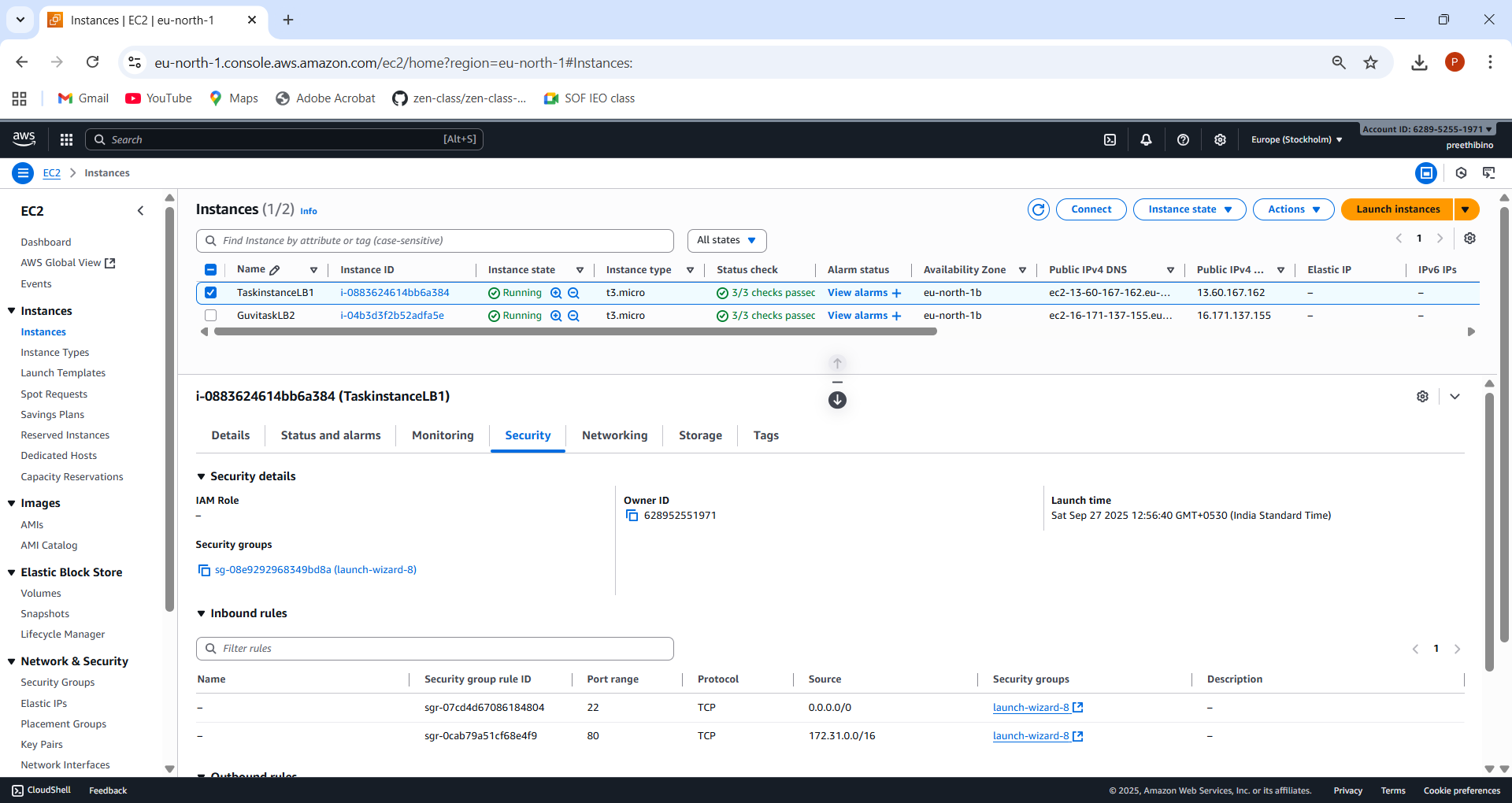
Create target group and attach both the instances

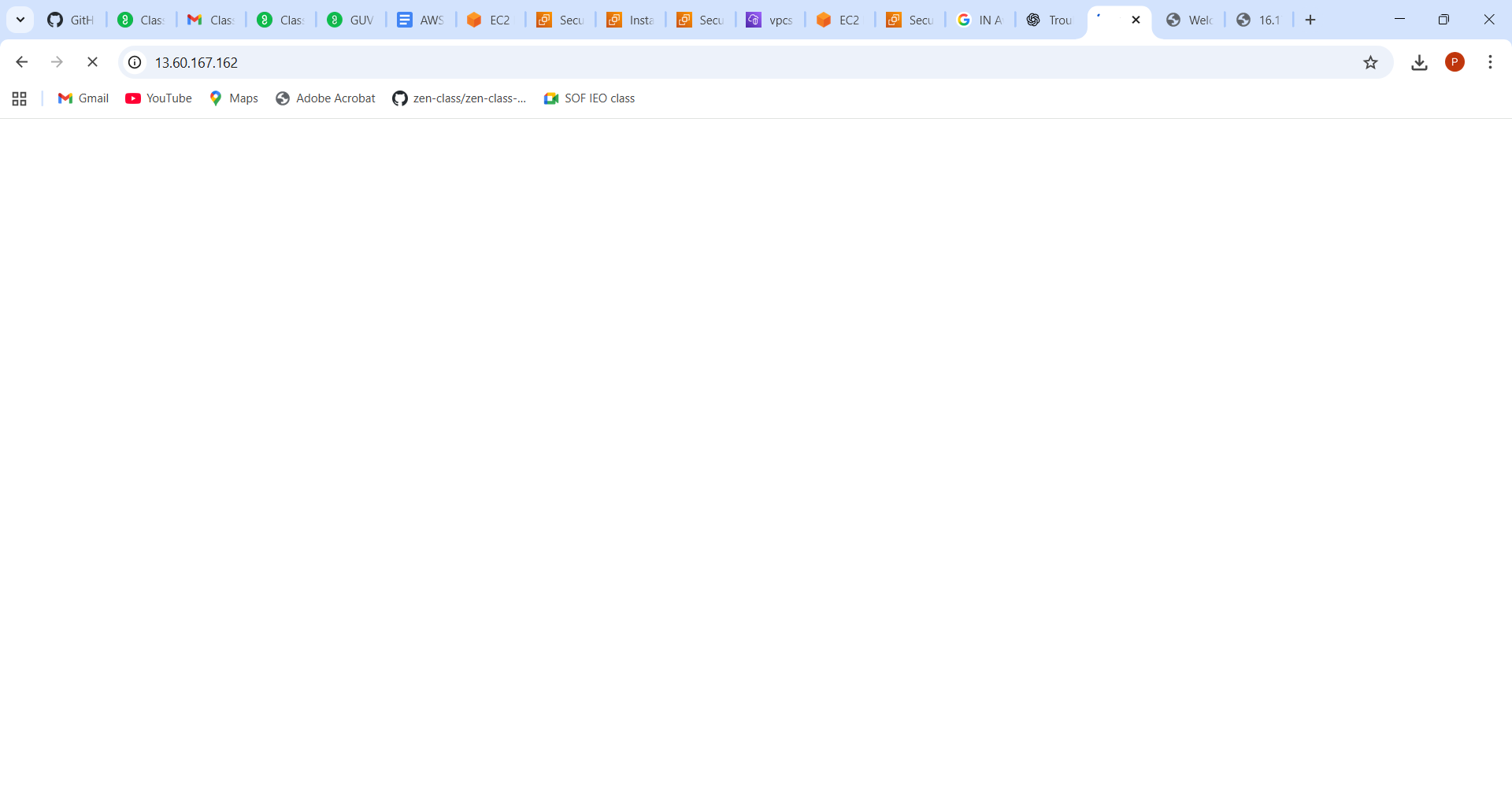


Create a load balancer and attach the target group

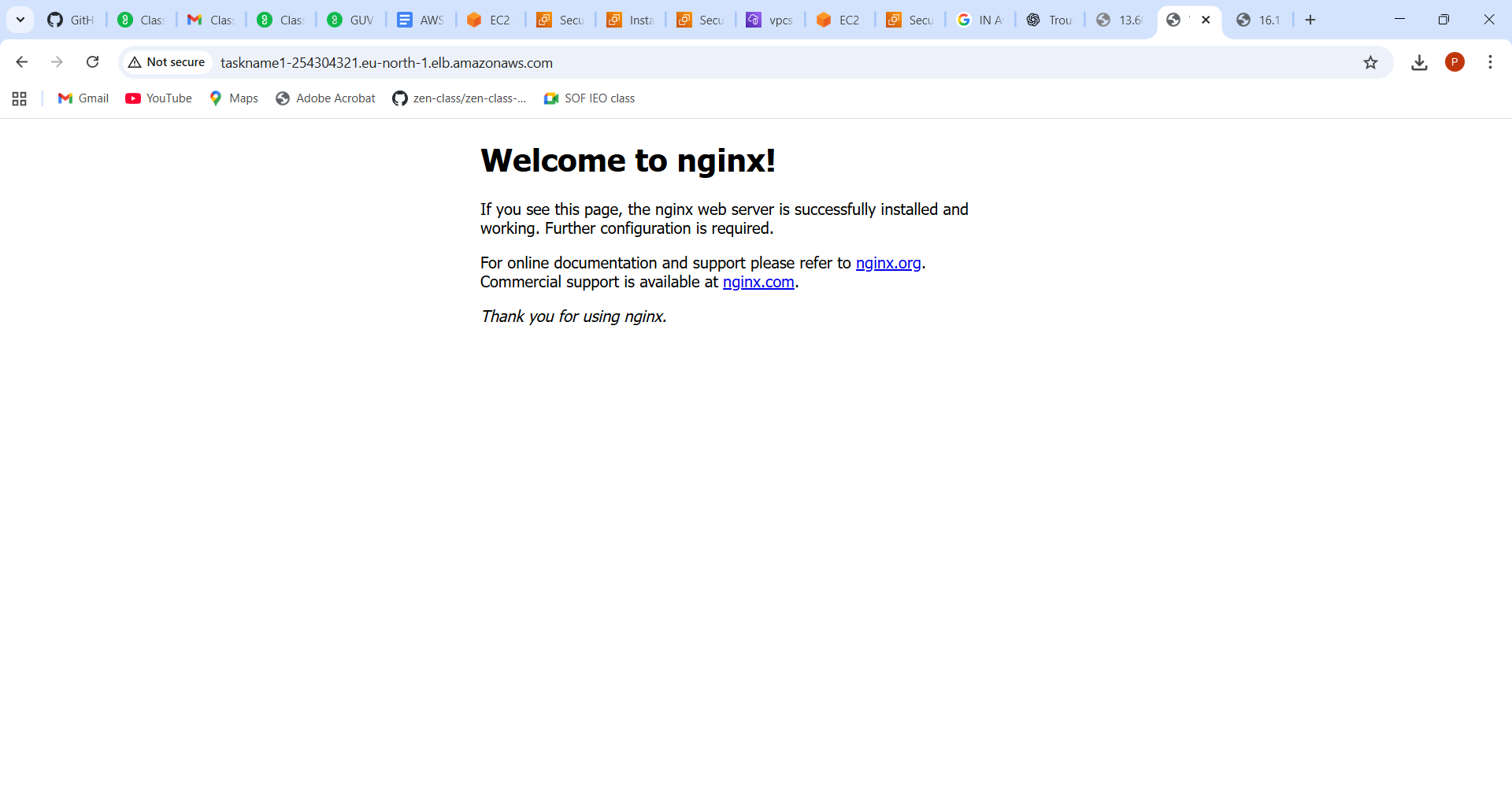


In Security group – point the load balancer in inbound rule

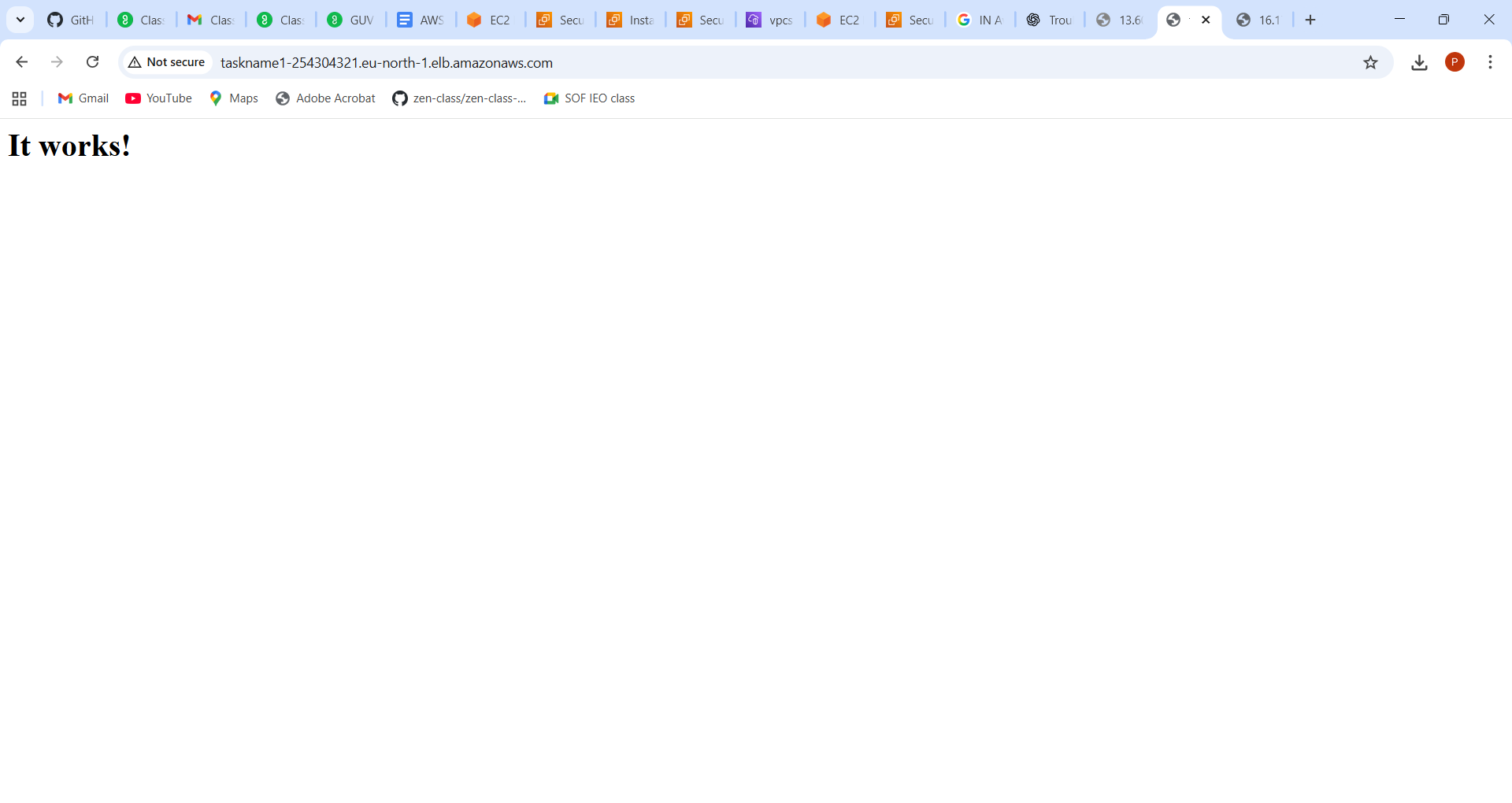


Using public IP- The nginx cannot be accessed 

Using load balancer DNS name, the load is balanced between ngnix and httpd



Second refresh



Notes for Self refernce:

1. Pointing VPC CIDR range in security group of EC2, ensures the public IP cannot be used for accessing applications
2. Use resource map in load balancer to identify, which part of the connection is unhealthy
3. If healthcheck is failing , adjust the healthcheck response code in healthchecks tab inside targetgroups