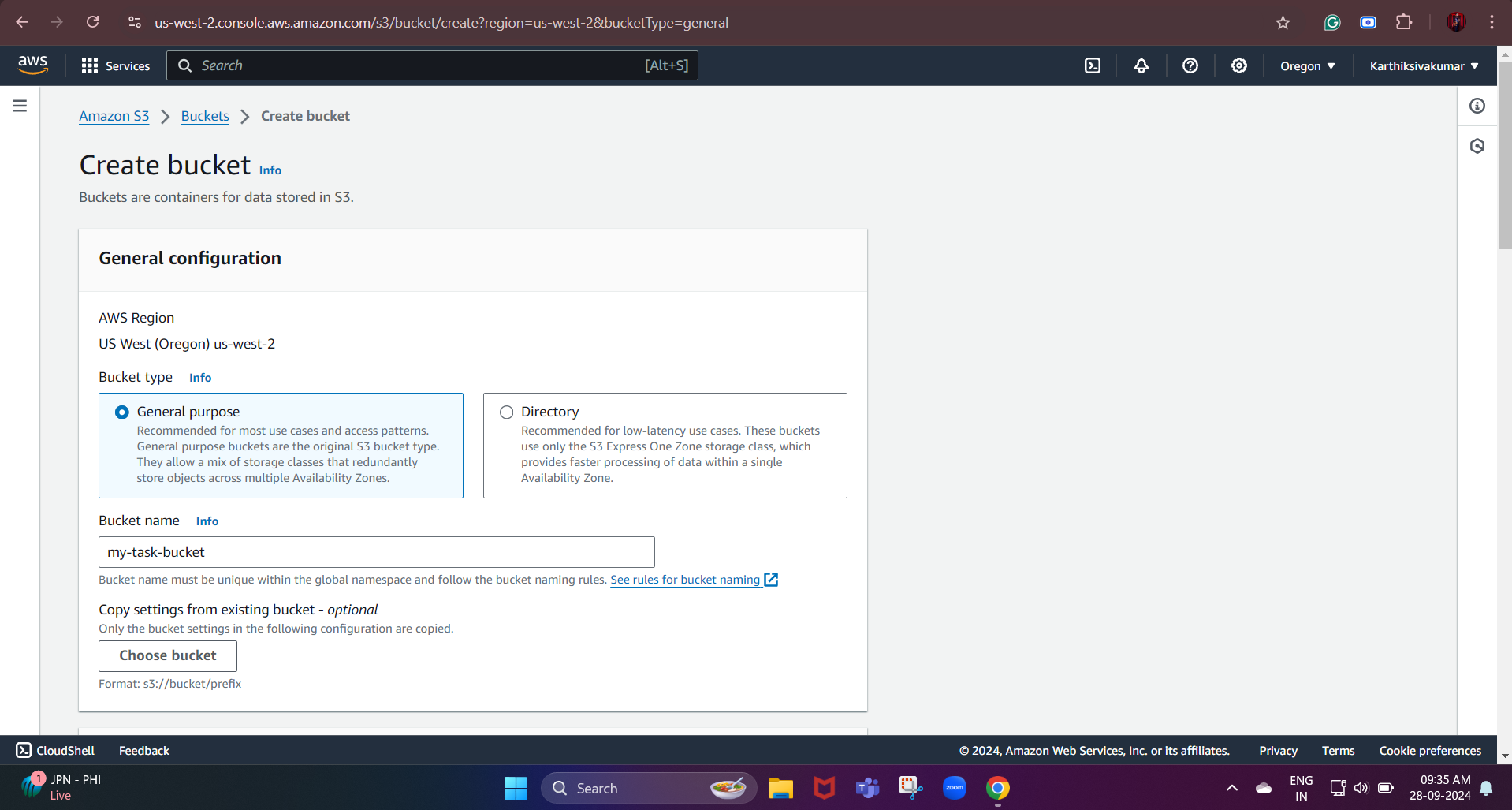
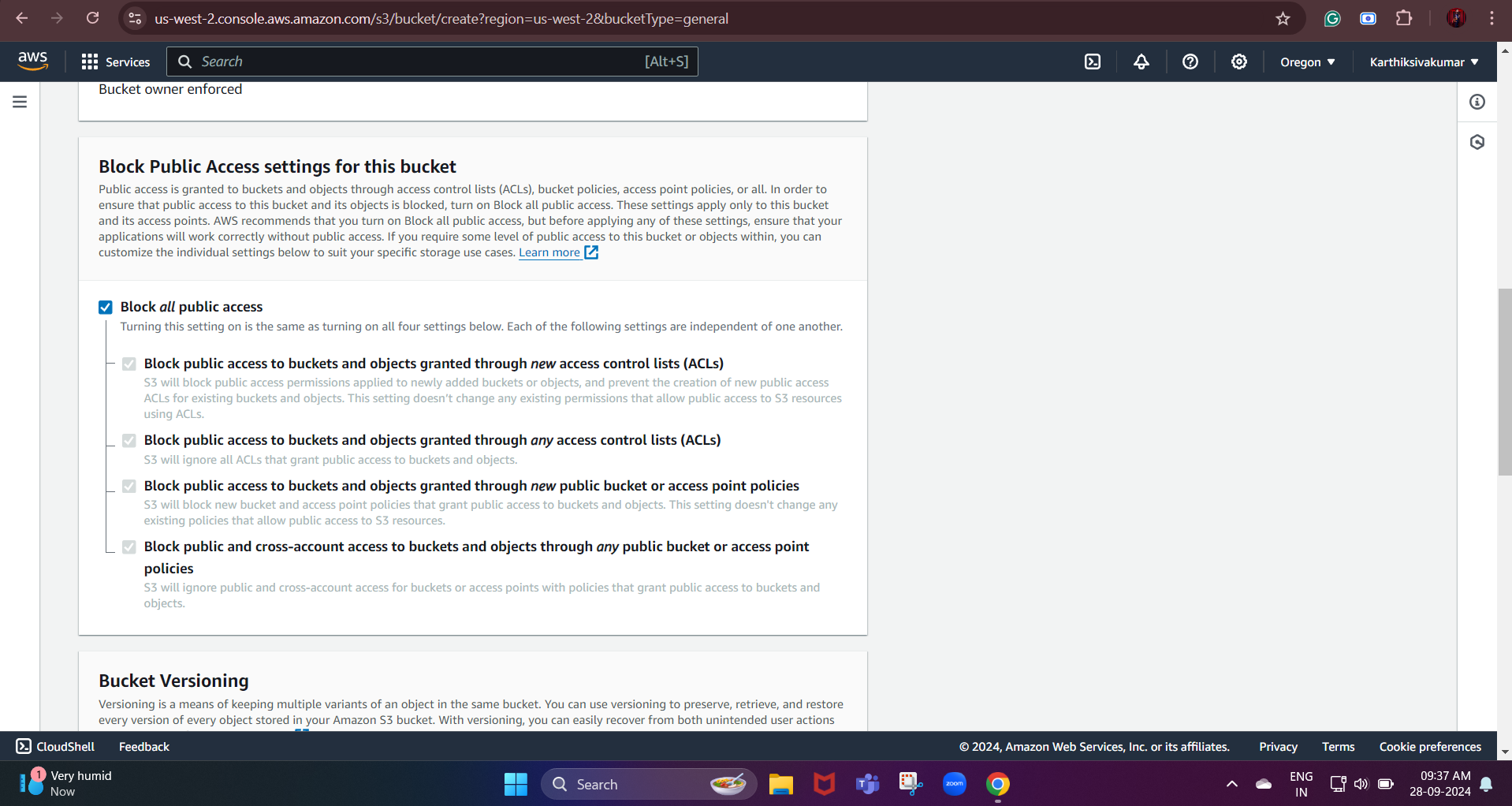
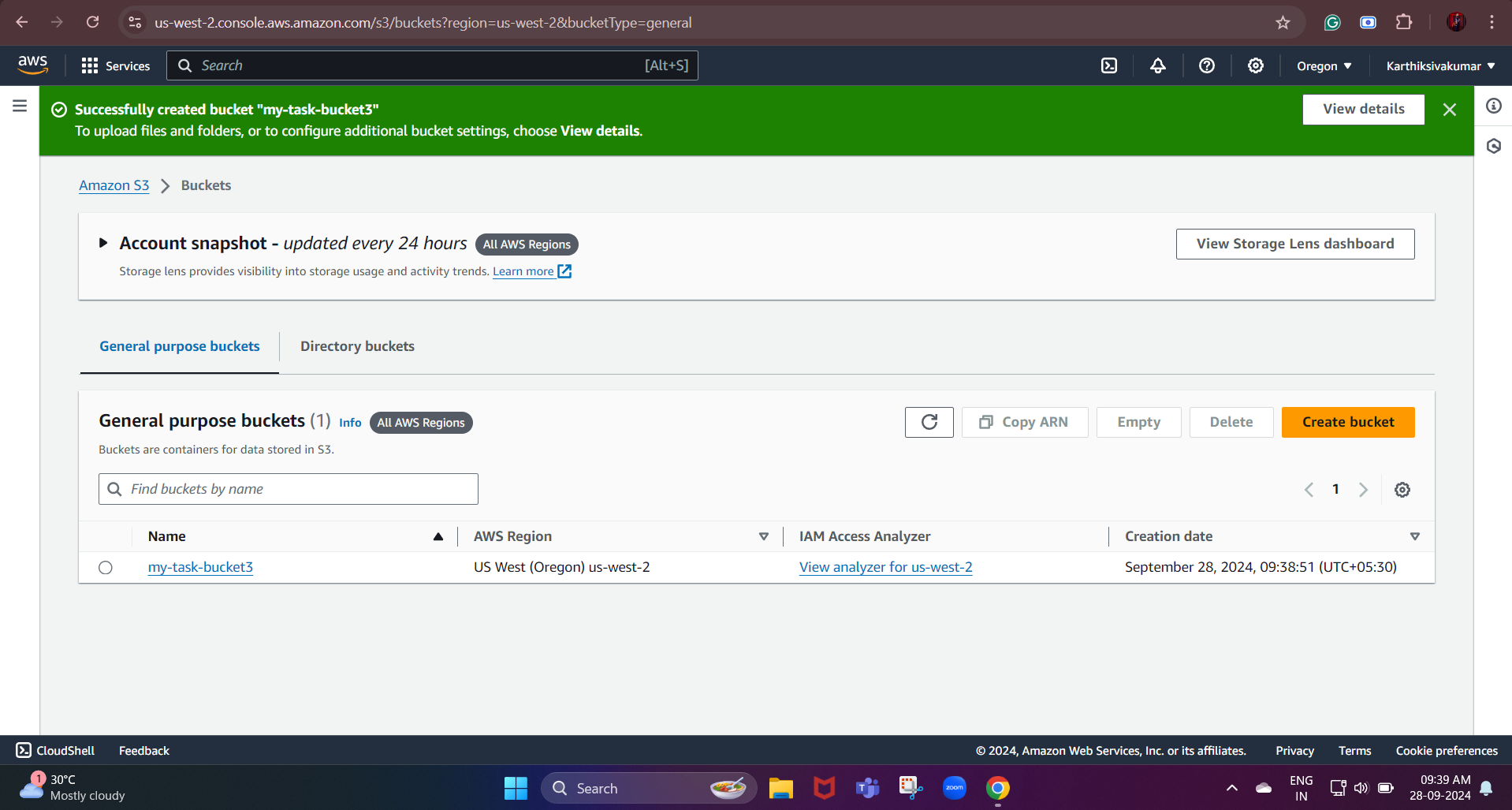
1. Create a S3 bucket, with no public access and upload files to the bucket & view the logs using Cloudwatch for the uploaded files.

First, we are going to create the bucket:



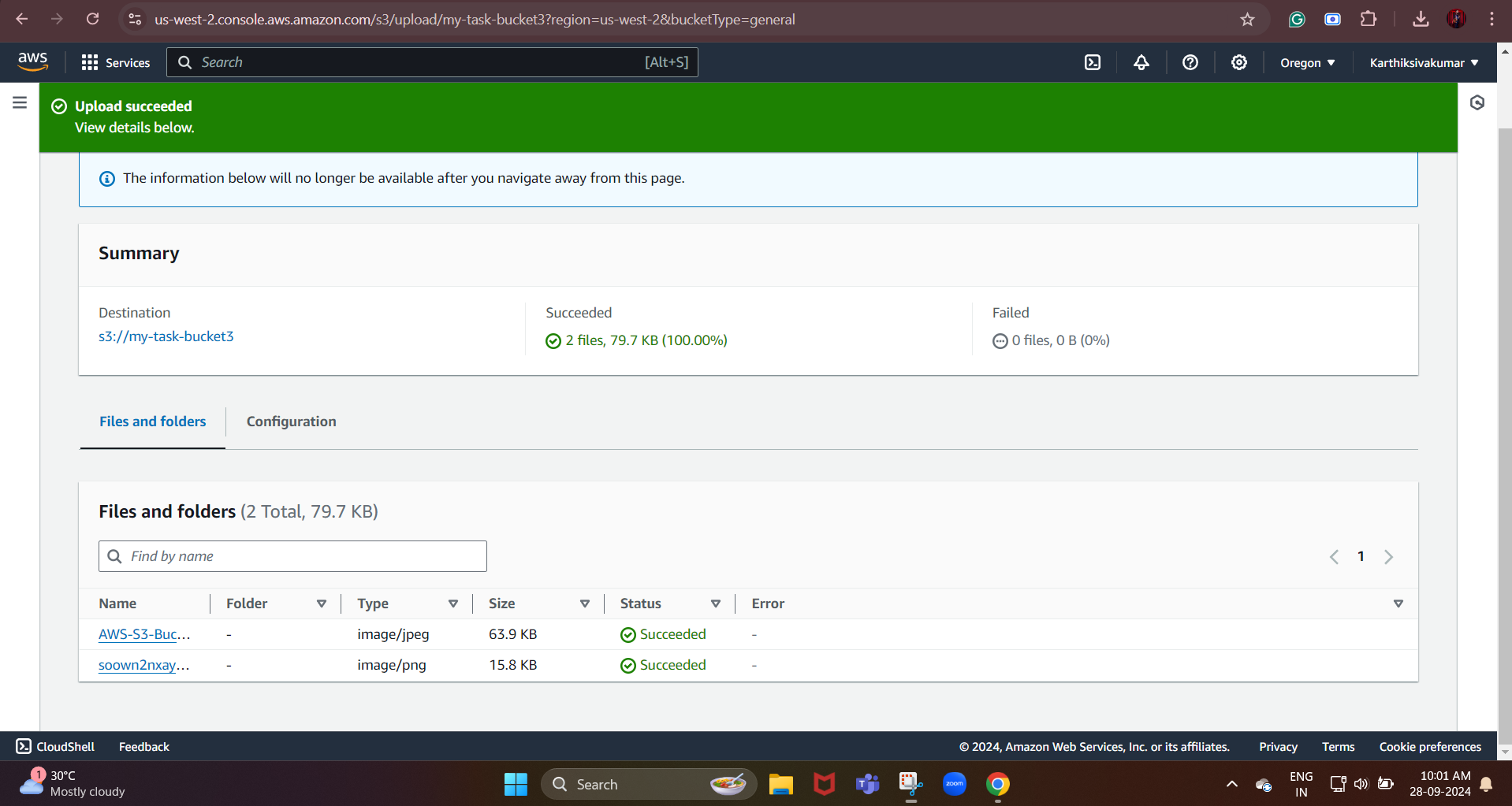
Then, we need to block public access:





Now, we need to upload the files in the bucket we created:

For that, we need to select the created bucket and click the upload option on that page.

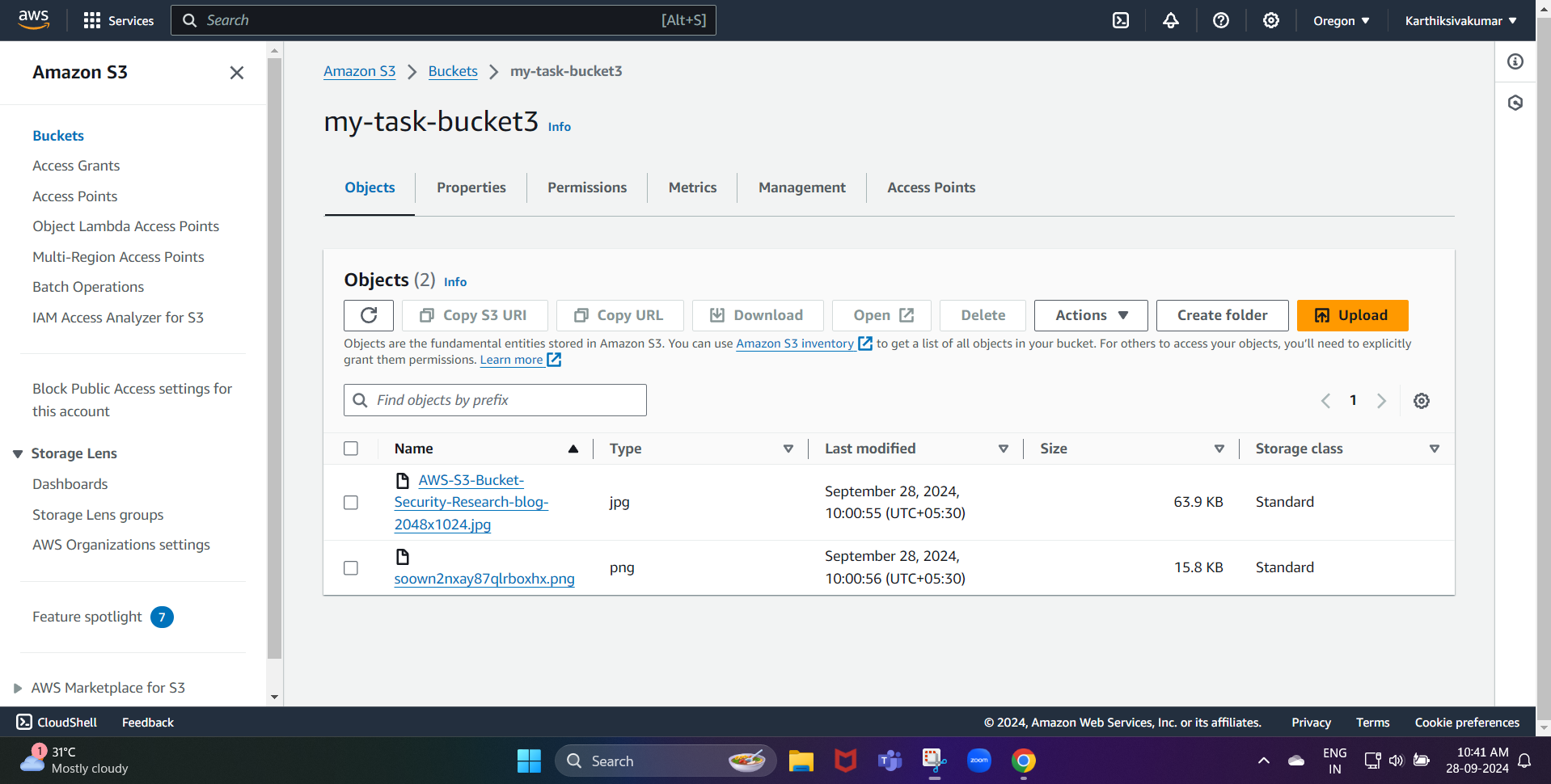


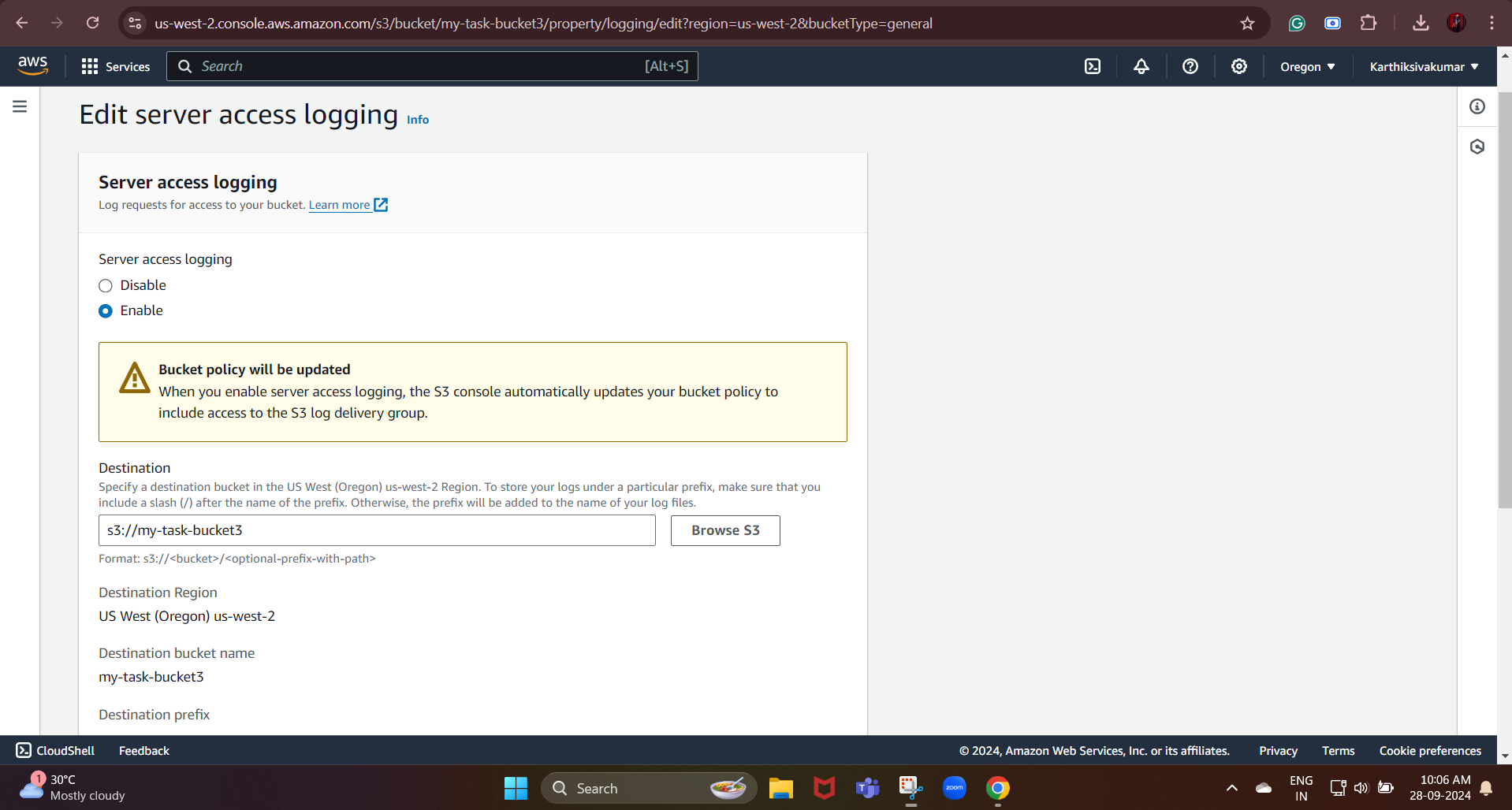
Now, the files have been uploaded to the bucket.

Next, we need to enable logging and cloud watch logging for S3:

Enable Logging for the S3 Bucket:

* We need to go to the properties tab
* In that, we need to scroll down to the server access logging section.
* In that, we need to click the edit option, and then we need to enable loggin.



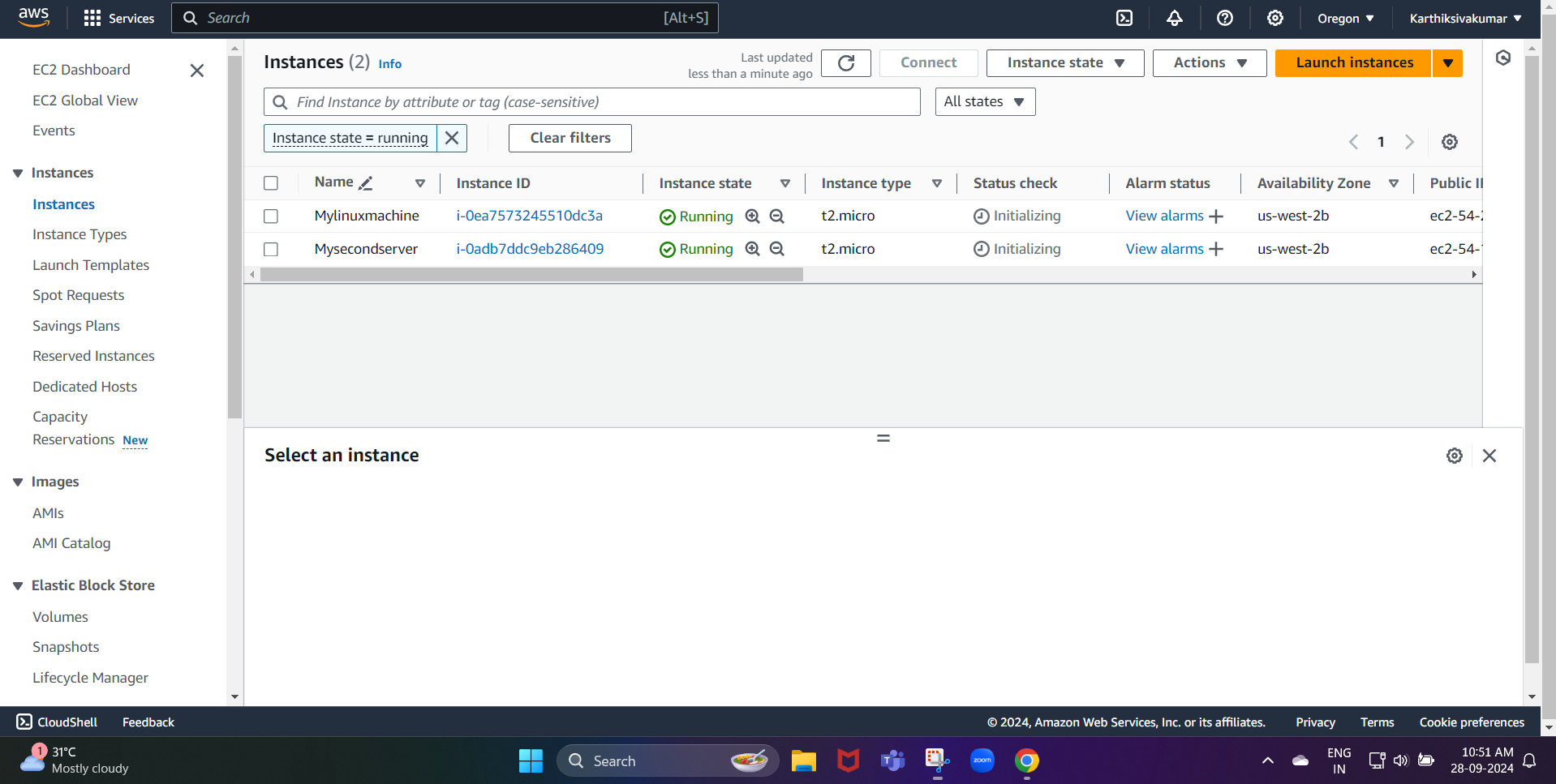


CloudWatch is a monitoring service for AWS resources and applications. CloudTrail is a web service that records API activity in your AWS account.

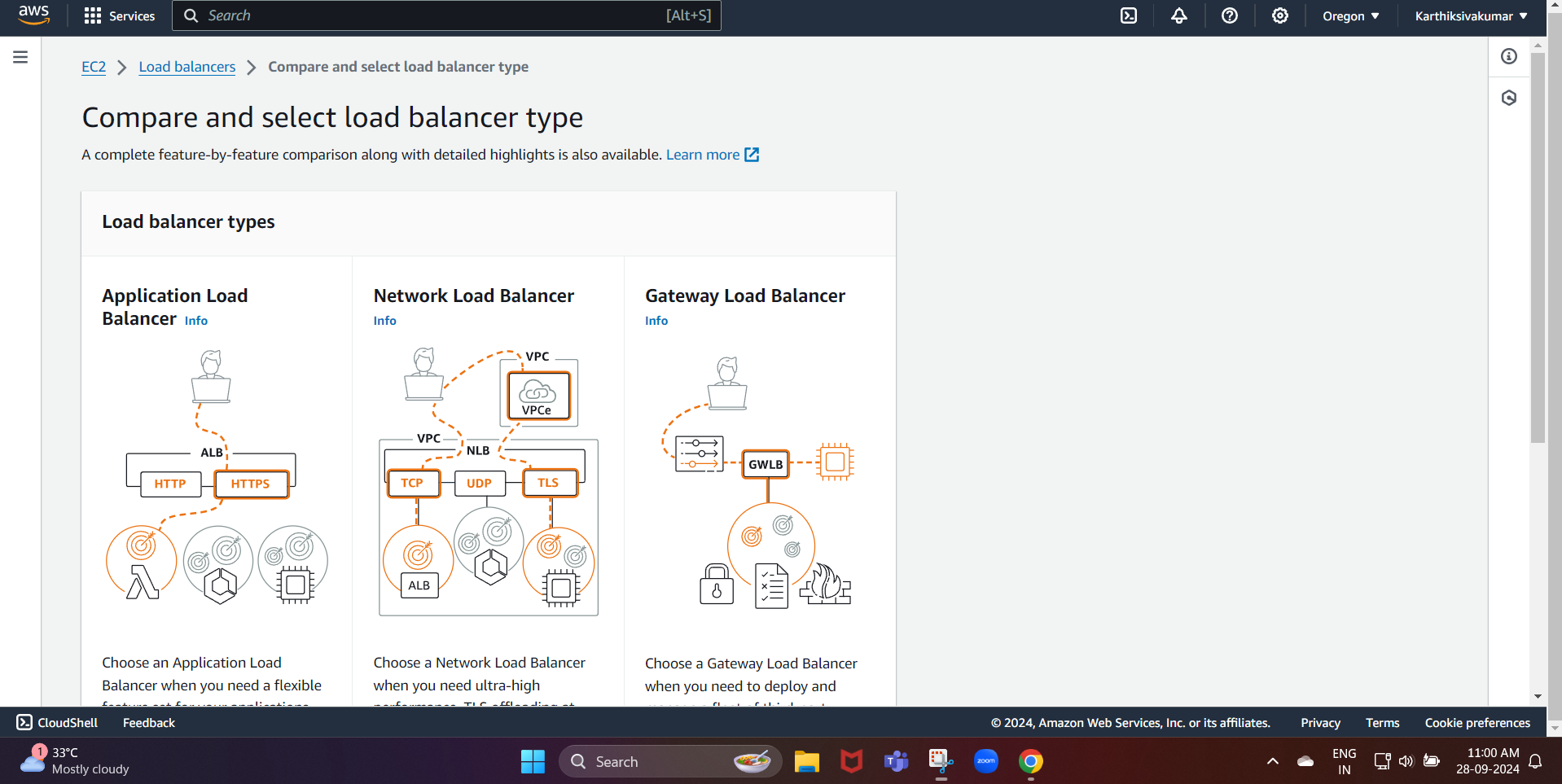
Enable CloudWatch Logging for S3 (CloudTrail)

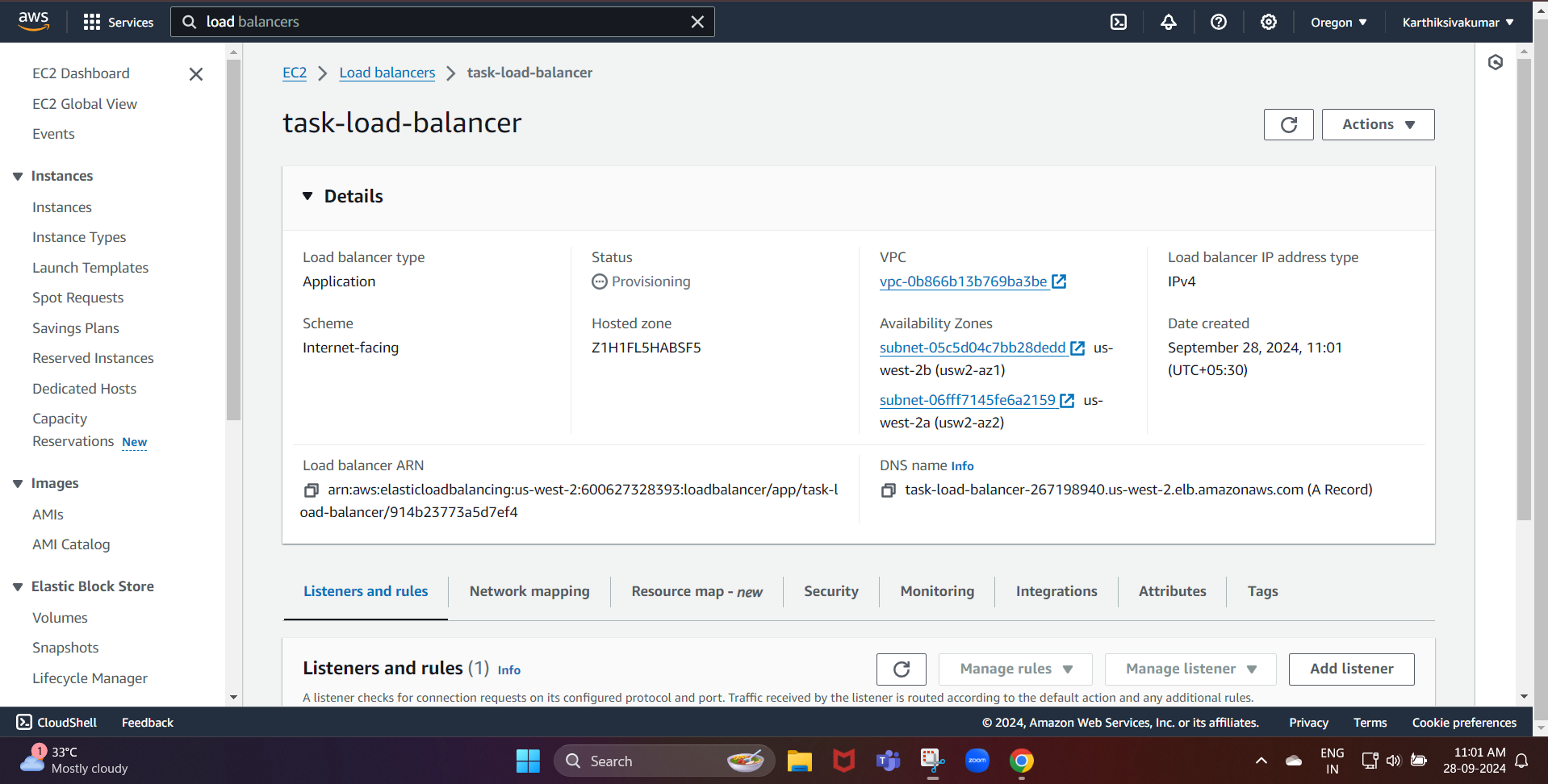
Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

First, we created two instances



Now, we need to create an application load balancer:





Now, we create the application load balancer

Next, we need to Update EC2 Instance Security Groups

Edit the security group to allow inbound HTTP traffic (port 80) from the ALB’s security group.

Make sure that the outbound rules in the security group allow traffic to all destinations (0.0.0.0/0) on required ports (like HTTP/HTTPS).

Route Traffic through the ALB:

First, we need to copy the DNS name from our ALB

task-load-balancer-267198940.us-west-2.elb.amazonaws.com

