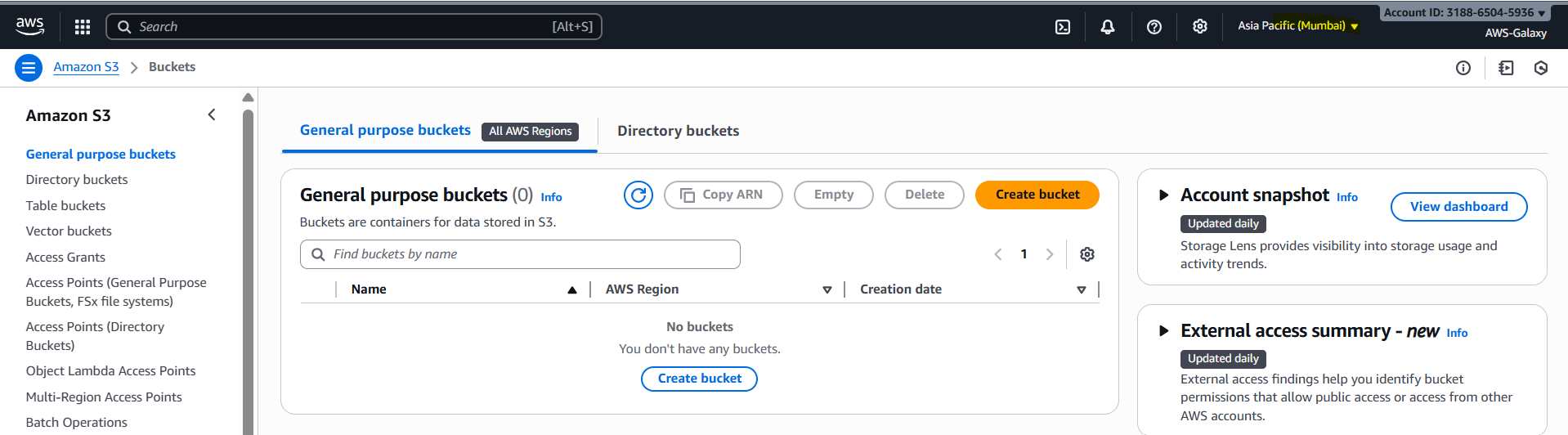
**Day 14: Sep 16h 2025:**

It is like google drive, under S3 we can store any kind of data. Images, videos, files etc…

S3 we can link to our running applications also.

It is ia global service. We can see all the S3 buckets of all regions at one place, there are not region or availability zone specific.

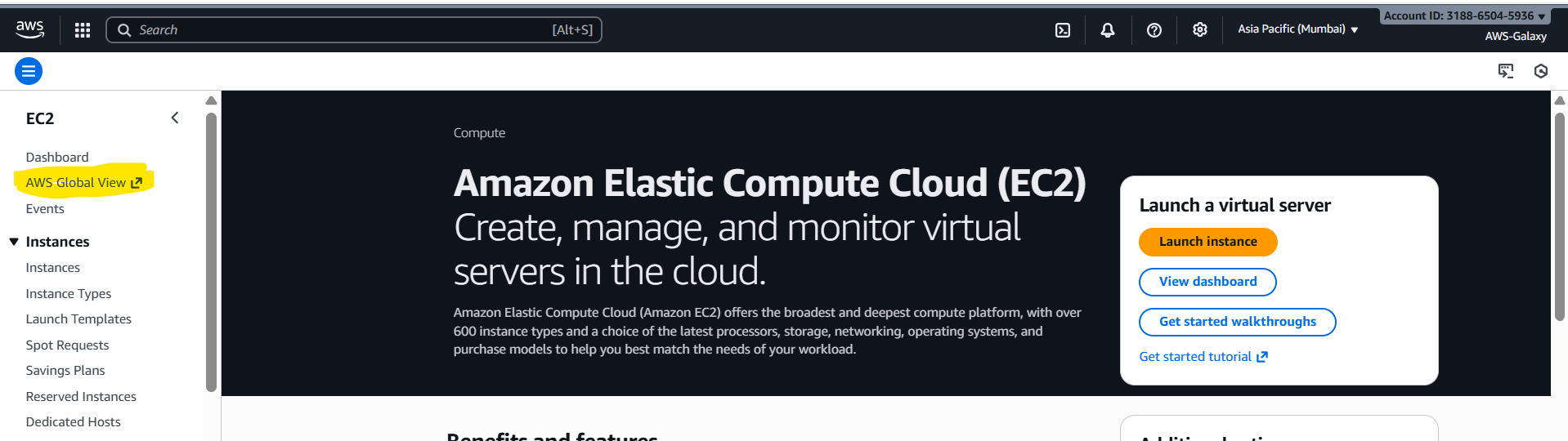
AWS 🡪 search 🡪 buckets 🡪 General purpose buckets 🡪 here we can see all regions related buckets.



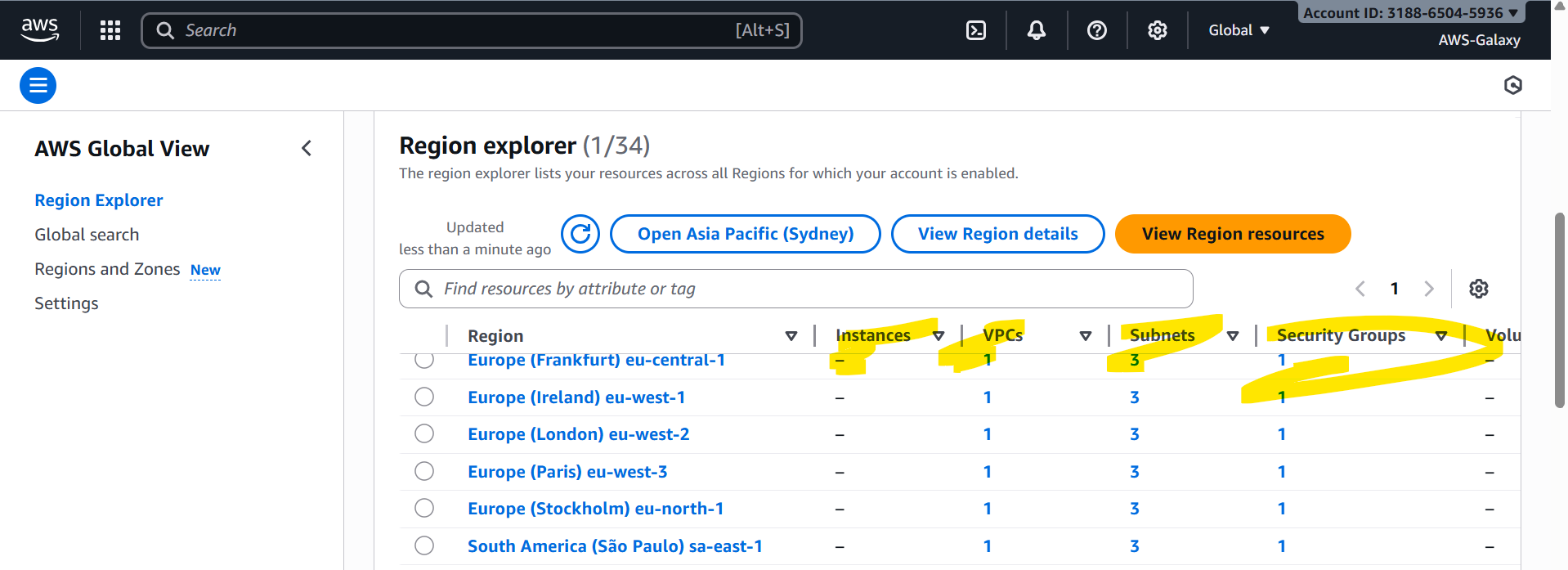
But in case of EC2 machines, if w want to see all Mumbai region EC2 machines we need to switch to Mumbai region, for other regions we need to switch but in case of S3 bucket we can see all buckets at one place.

EC2 also have global view means all EC2 machines we can see it one place.

AWS 🡪 EC2 -> “AWS Global view” 🡪 it will open new Window 🡪 here we can see all counts of Ec2 machines in all regions.



In new window we can see like below.



It will show only count, but it will not tell the EC2 machines are active, inactive, closed or terminated etc.

This global view sometimes not accurate, we better check EC2 machines in AWS🡪 EC2 🡪 instances console only.

The data we saved in S3 buckets are called as Objects. It is very rare to loose data from S3 bucket.

We can store unlimited data in S3 bucket. One file maximum size can be 5TB. We cant upload more them 5TB for single file.

Uploading file in S3 can be done in multiple ways.

1. Console which uses GUI. [<= 160GB we can upload in single attempt]
2. CLI / power shell. [5GB – 5TB]
3. Winscp [<= 160GB we can upload in single attempt]

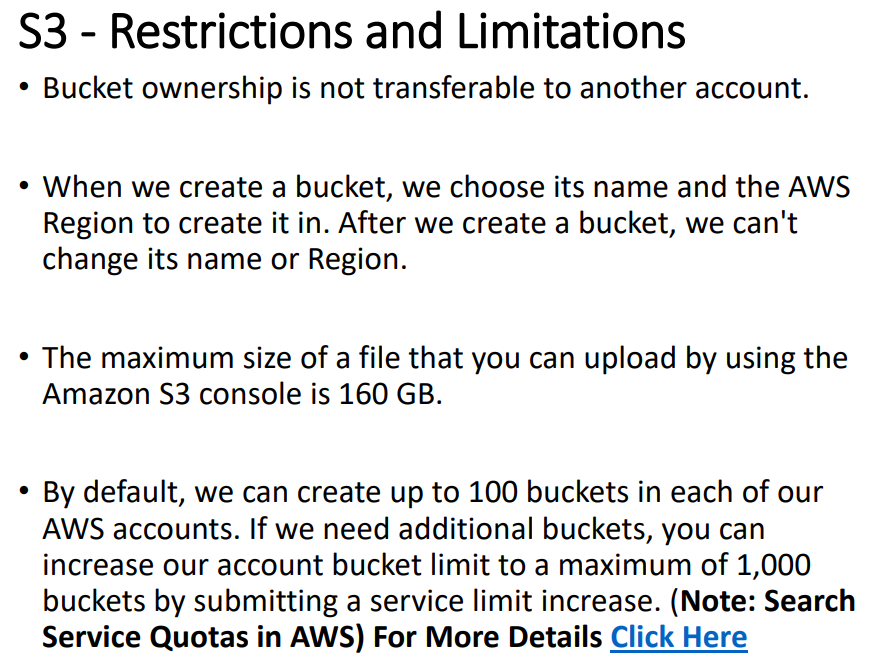
If we are uploading files using CLI or power shell then file size should ne 5GB – 5TB in this case S3 will use technology uses “multipart” upload. Here they will make our big file into small small parts and then after sending it will make as single file. This process will happen in backend.

By using console or WINSCP we can’t upload a file which size more than 160GB.

While creating S3 bucket, its name we should give unique globally. Like creating Gmail.

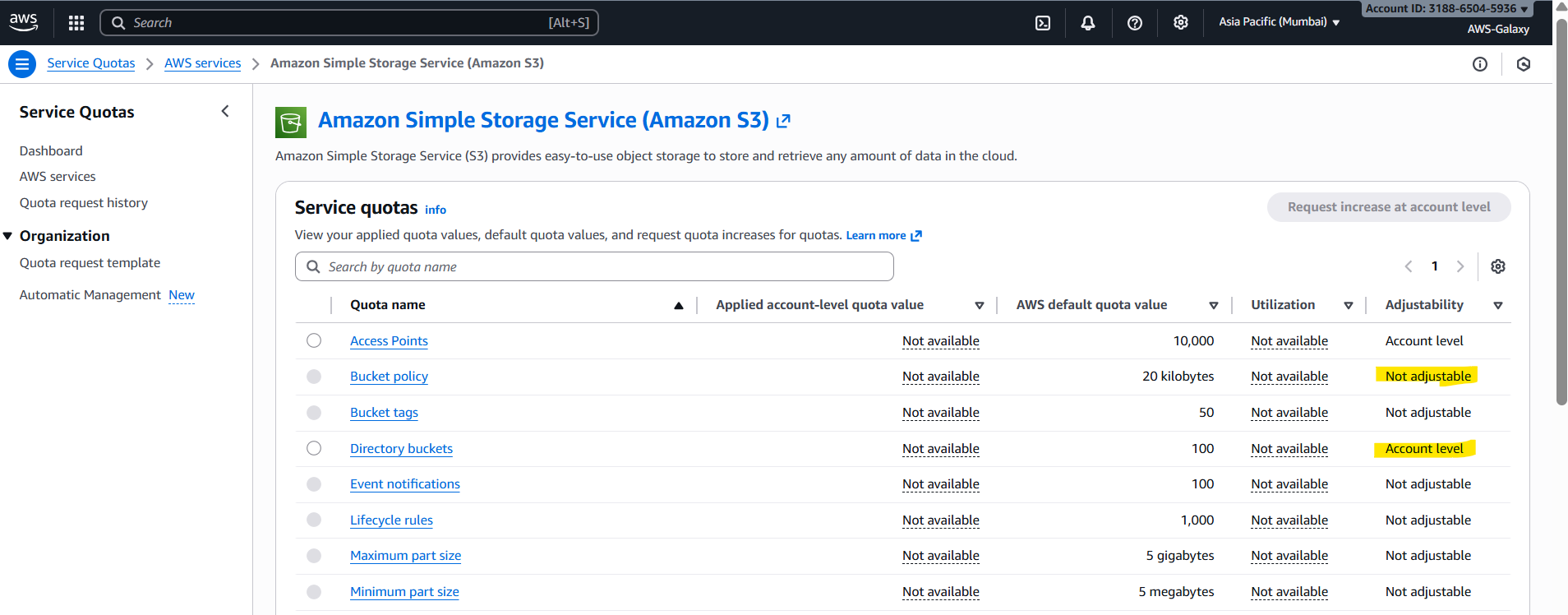
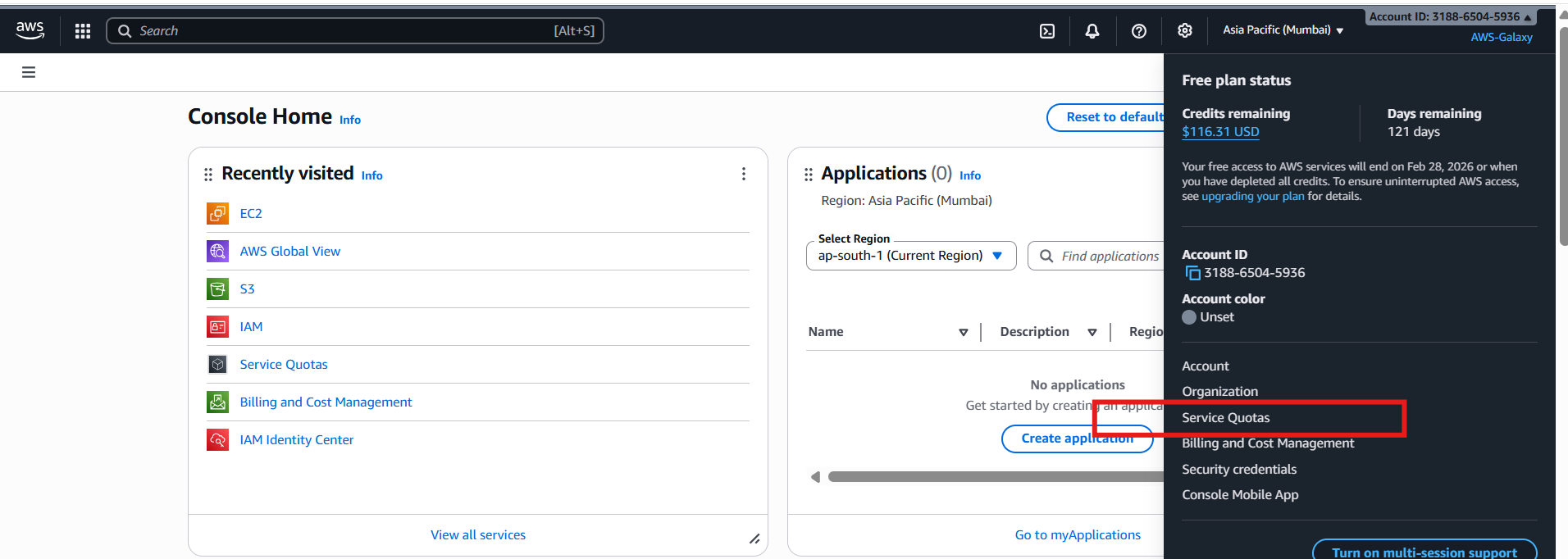
We are going to learn further.

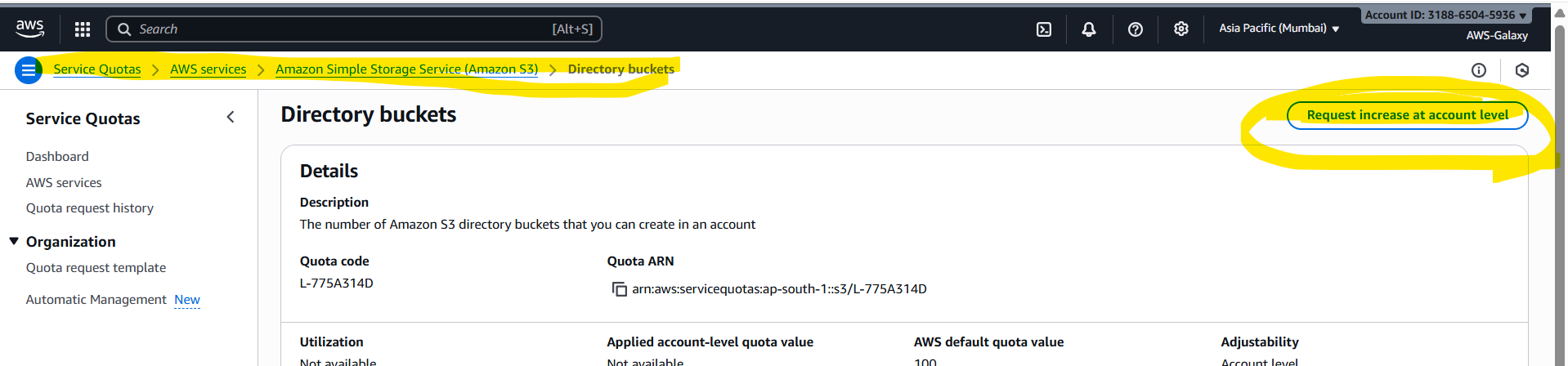
1. S3 bucket life cycle management.
2. Versioning.
3. Encryption.
4. Securing S3 bucket using ACL (Access Control List) and bucket policies.

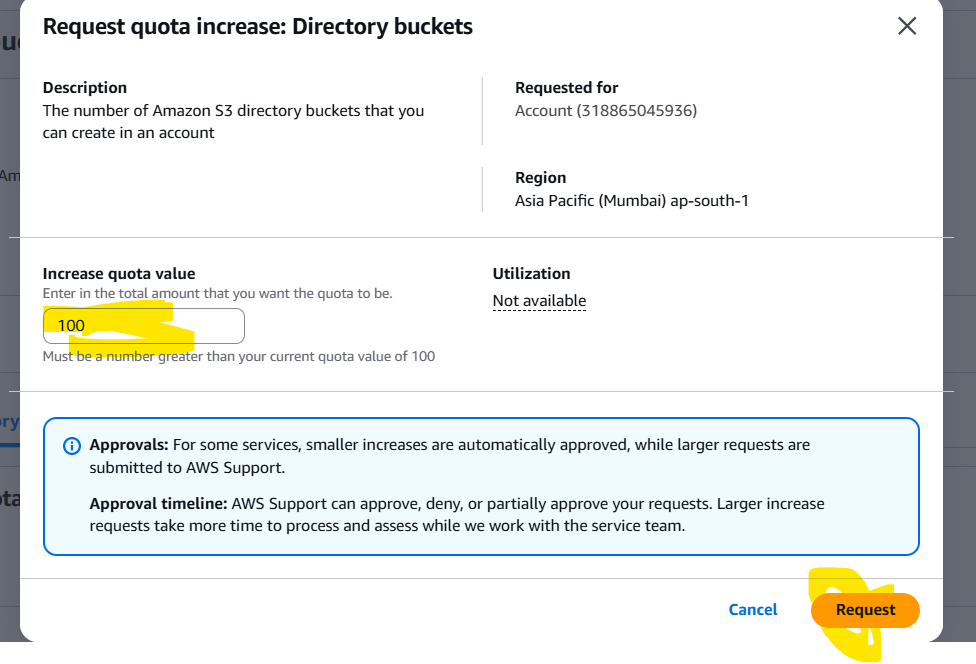


“Service Quota” – Is used to increate the limit of creating S3 buckets. Not only for S3 for all AWS services it can be used.

We can see this option in name menu option. AWS 🡪 right side top corner 🡪 click on Name menu 🡪 Service Quota.--> it will open new Window 🡪 AWS services 🡪 search for S3 🡪 Amazon Simple Storage Service (Amazon S3) 🡪 search for “Directory buckets” 🡪 click on that 🡪 riht side “Request increase at account level”.

We can see Not adjustable and account level, not adjustable mean we can not increase the limit. 

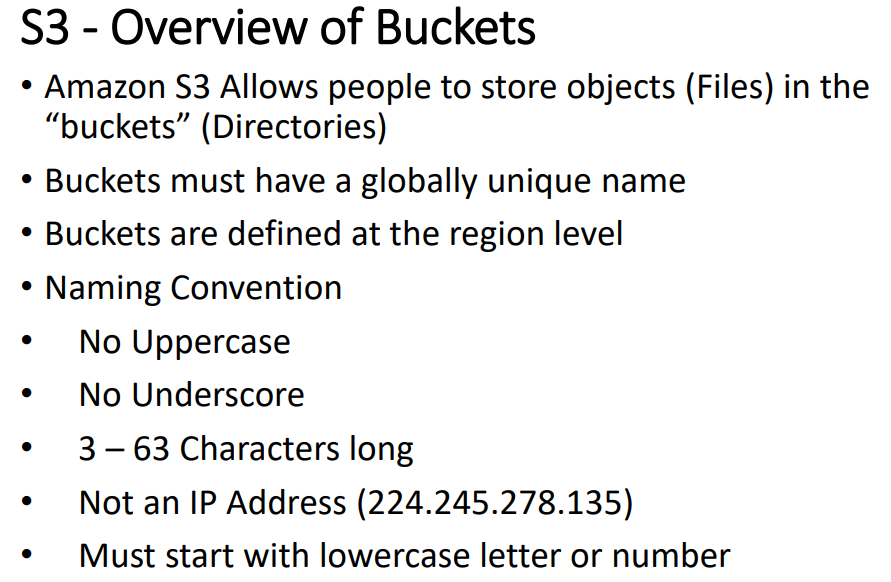




By default it is giving it is 100, we can increase as per our requirement.

Under Free tier 5GB of data we can store in S3 bucket.

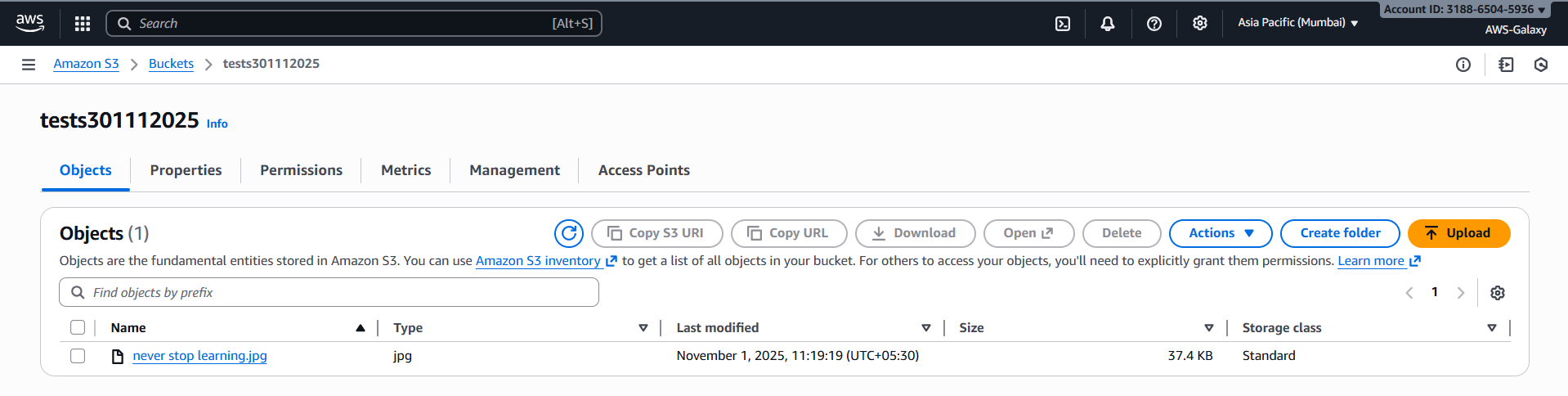
By using “service quota” we can increase the limit of any service.



AWS 🡪 S3 🡪 name should be globally unique 🡪 ACL enabled 🡪 uncheck “Block all public accesses” (means we are giving public access to our S3 bucket) 🡪 tick the check box “ I acknowledge that the current settings… “ 🡪 don’t fill anything 🡪 click on “ Create Bucket”.

Next target is to upload files to created S3 bucket.

AWS 🡪 s3 🡪 open our bucket --> upload 🡪 add files 🡪 browser and add files 🡪 Permissions tab 🡪 select the radio button “**Grant public-read access**” 🡪 tick the check box “I understand the risk of …” 🡪 click on “Upload” button.



**Now how to access the file that we have uploaded.**

AWS 🡪 S3🡪 bucket 🡪 click on filename 🡪 **Object URL** 🡪 copy… past that URL on any browser URL and access.

Anyone can access this file as we have given public access to this object.

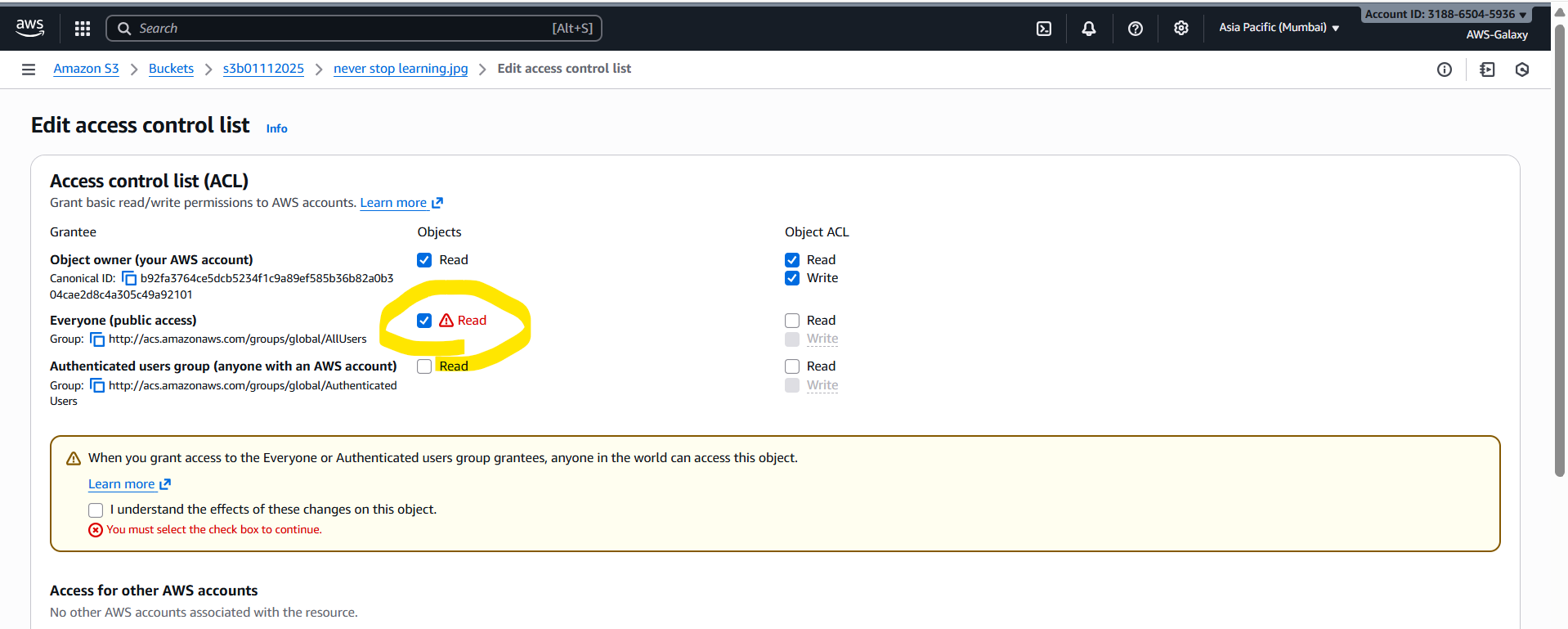
In above case we have given public access at bucket level and object level also.

For any file we uploaded for all files we will get one URL.

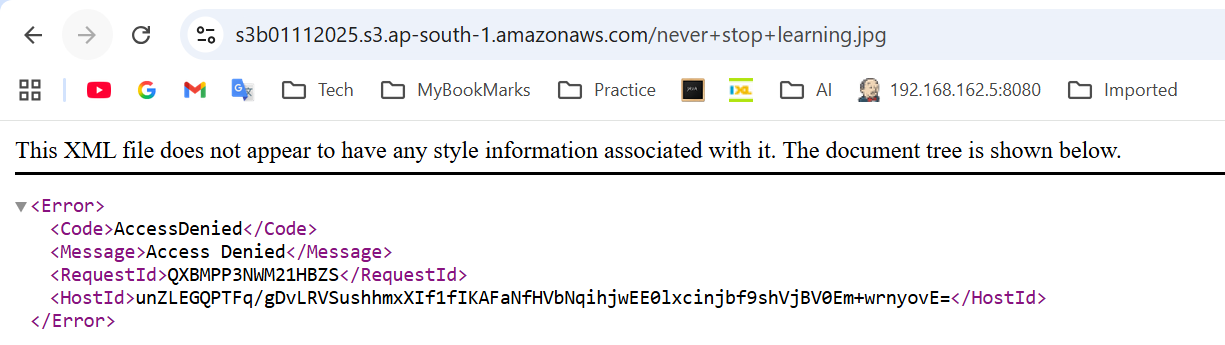
Please go through all options it provides.

**How to remove public access to object we uploaded?**

Click on Our s3 bucket 🡪 click on our object we uploaded 🡪 Permissions tab 🡪 Edit 🡪 uncheck “**Everyone (public access)**” 🡪 click save changes button.



Now if we try to access Object URL in the browser we are going to get below error.

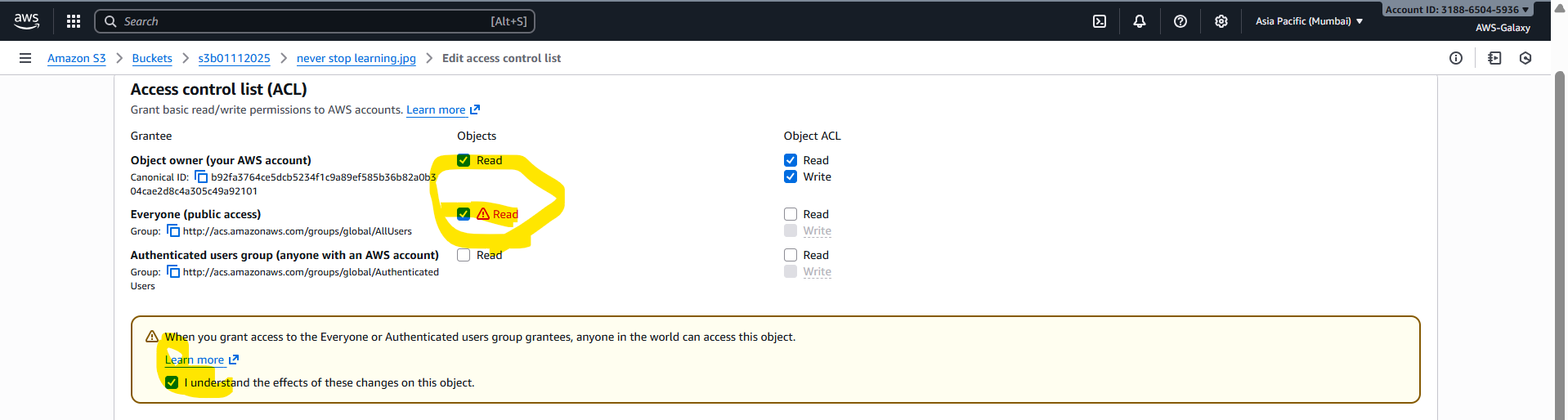


Now our next task is to give public access to object we uploaded and removing the public access to bucket we created.

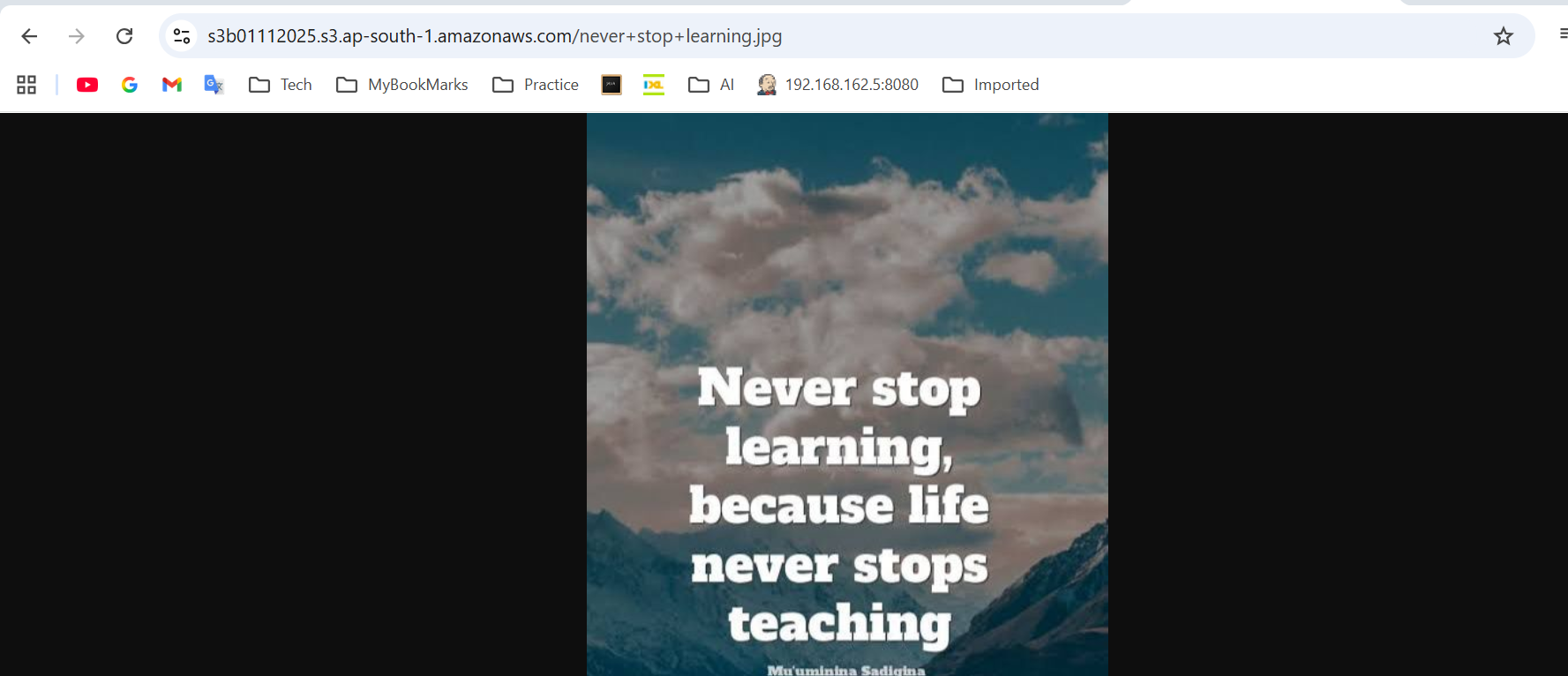
1. How to add back public access to object we uploaded?

How we removed public access reverse way we need to provide public access by tick the check box.

Click on Our s3 bucket 🡪 click on our object we uploaded 🡪 Permissions tab 🡪 Edit 🡪 uncheck “**Everyone (public access)**” 🡪 click save changes button.

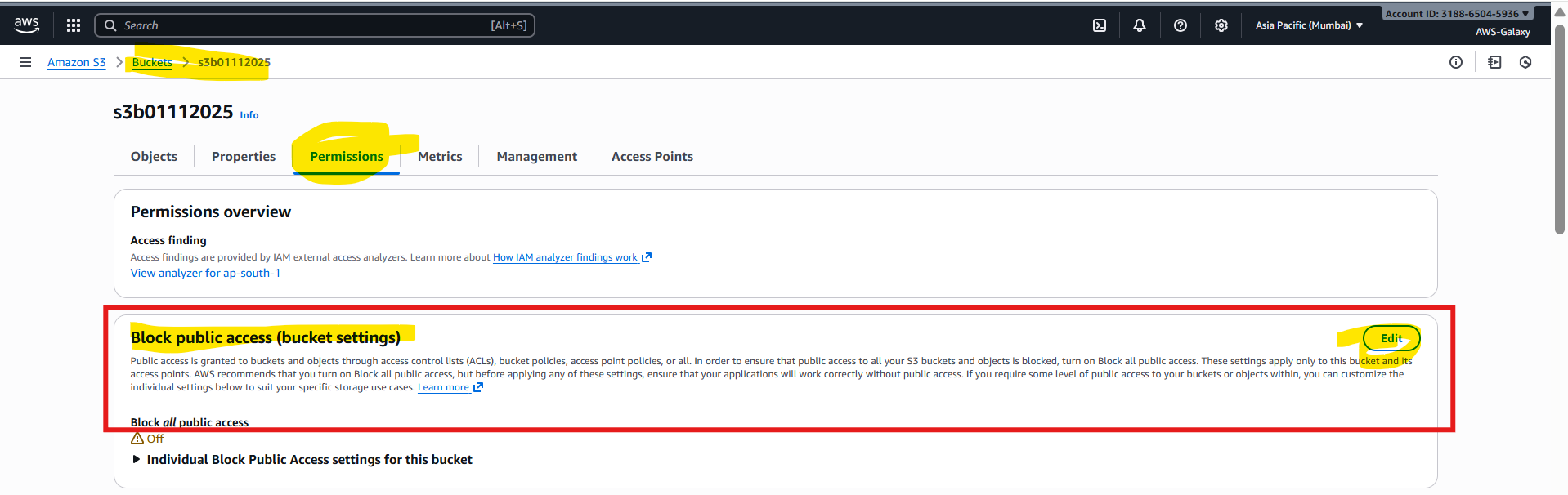


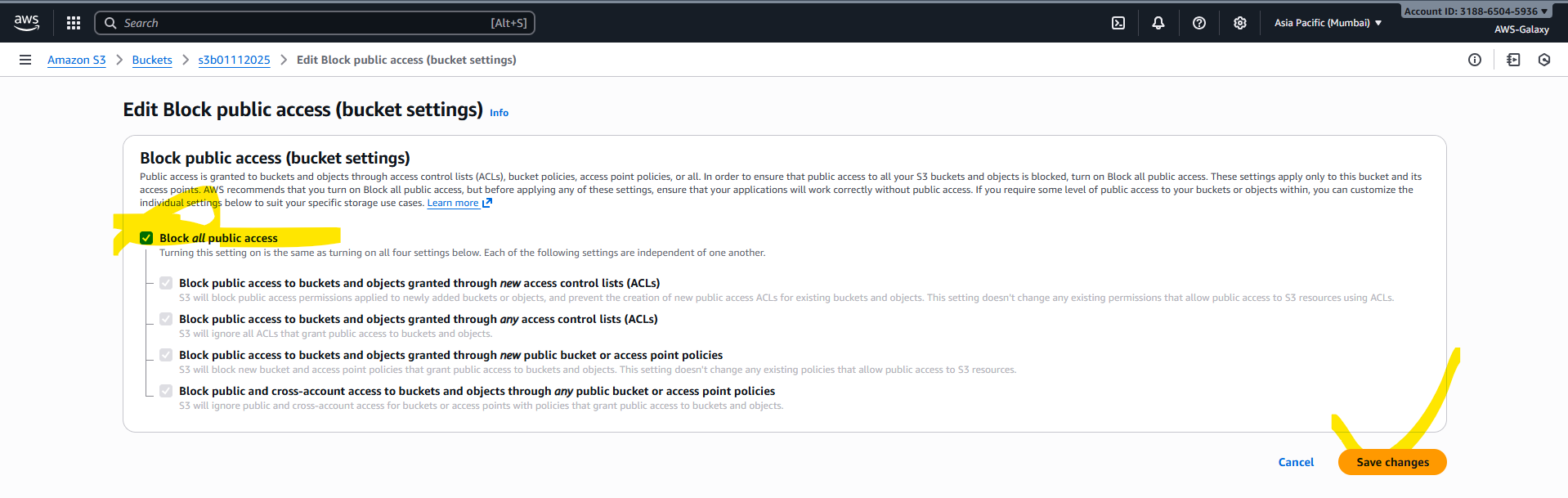
Now if you access the Object URL in the browser we can see the uploaded image.

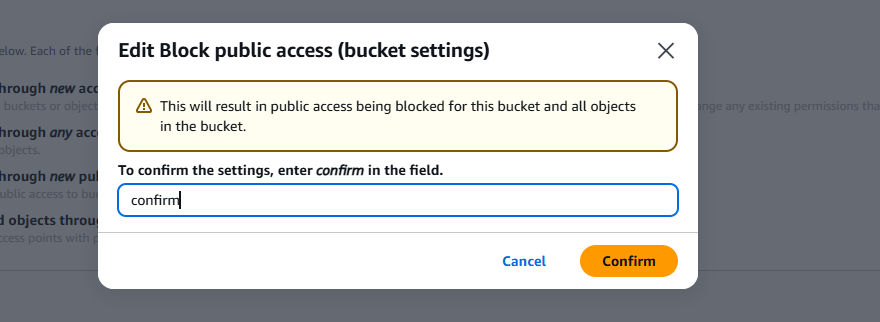


1. Now remove the public access to the bucket we removed.

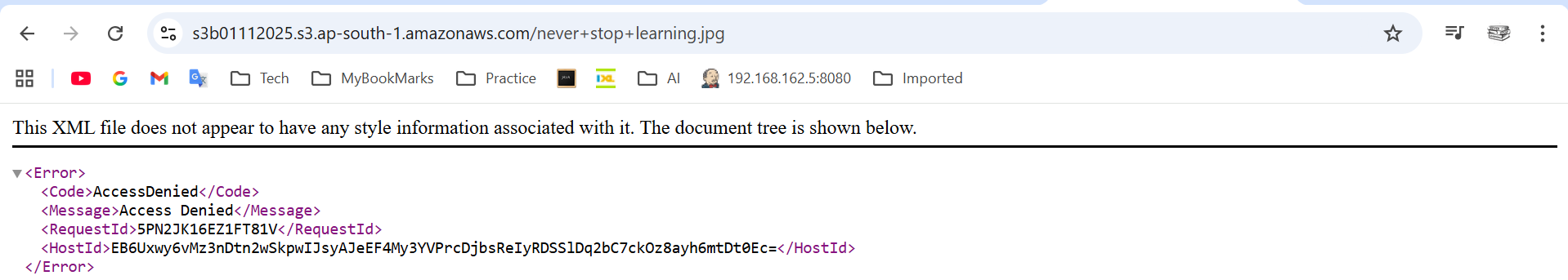
Click our S3 bucket 🡪 permissions 🡪 Block public access (bucket settings) 🡪 tick “Block all public access” 🡪 save changes. 🡪 confirm popup.







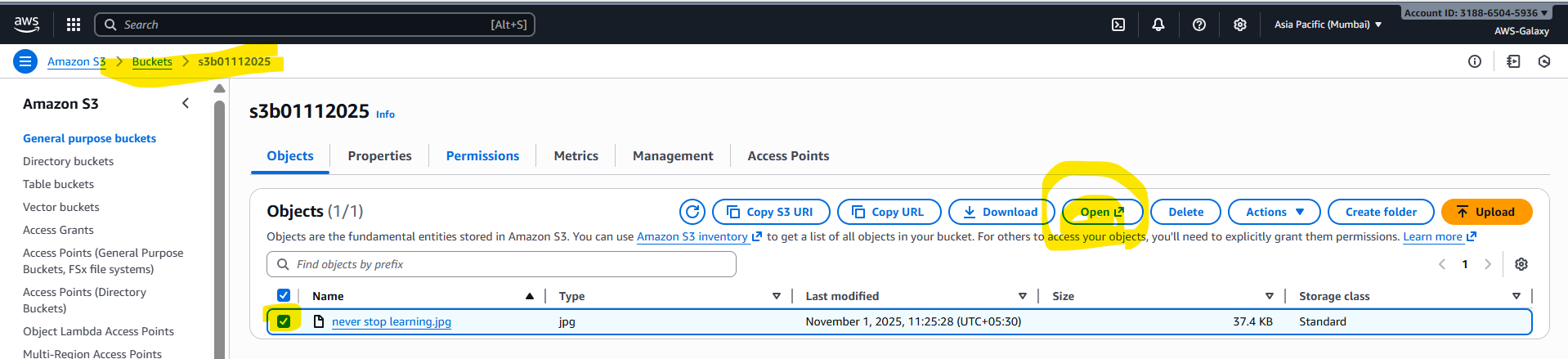
Now if we try to open object URL again we are going to get error on browser.



Means without public access other can not access objects inside the S3 bucket. But we can access as we are created.

How to object from S3 if it is non-public.

Our S3 bucket 🡪 select the image 🡪 click on Open button. It will open in separate browser tab.



After practice please delete all S3 buckets you created.

How to delete S3 bucket we created?

Before deleting s3 bucket we need to delete objects inside it. Then only it will allows us to delete s3 bucket.

