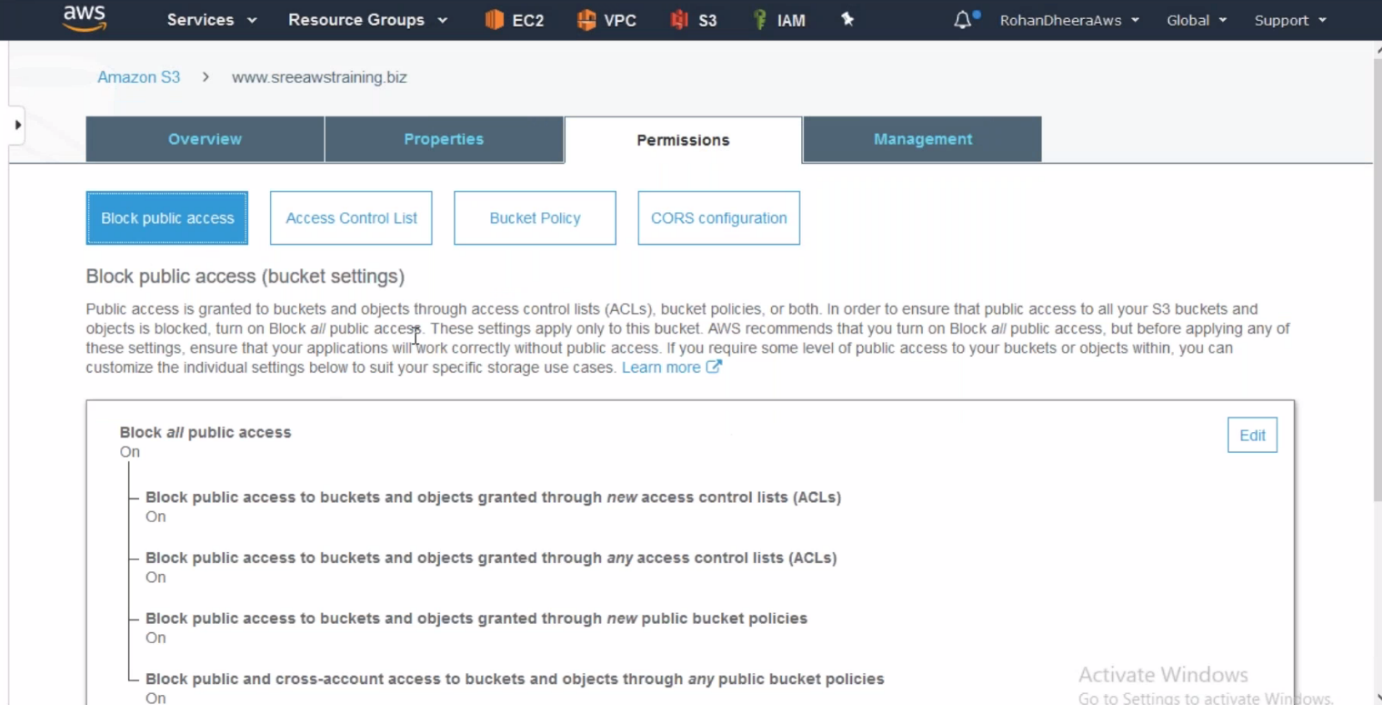
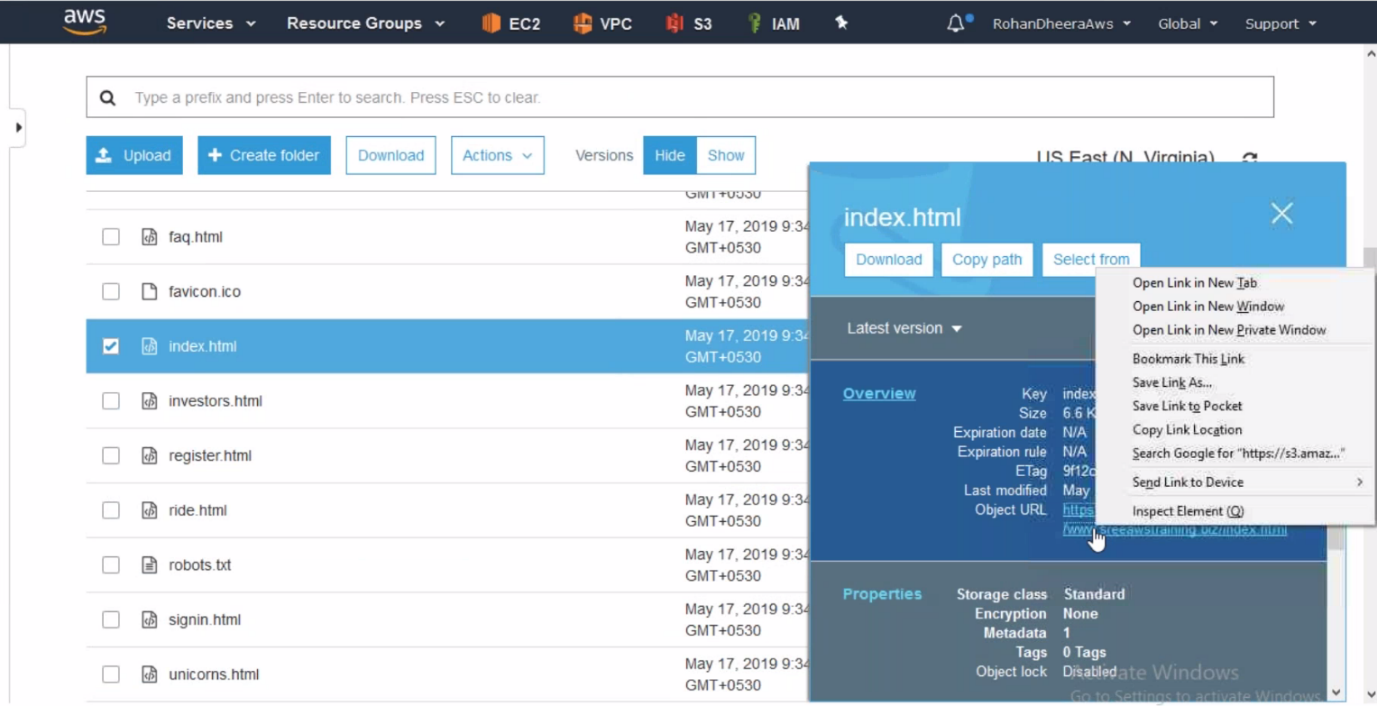
**20.AWS-S3-Part-2**

**PERMISSION**

**Block All Public Access**

If you enable BLOCK ALL PUBLIC ACCESS, you cannot access the content in s3 through internet. It will give permission denied error.





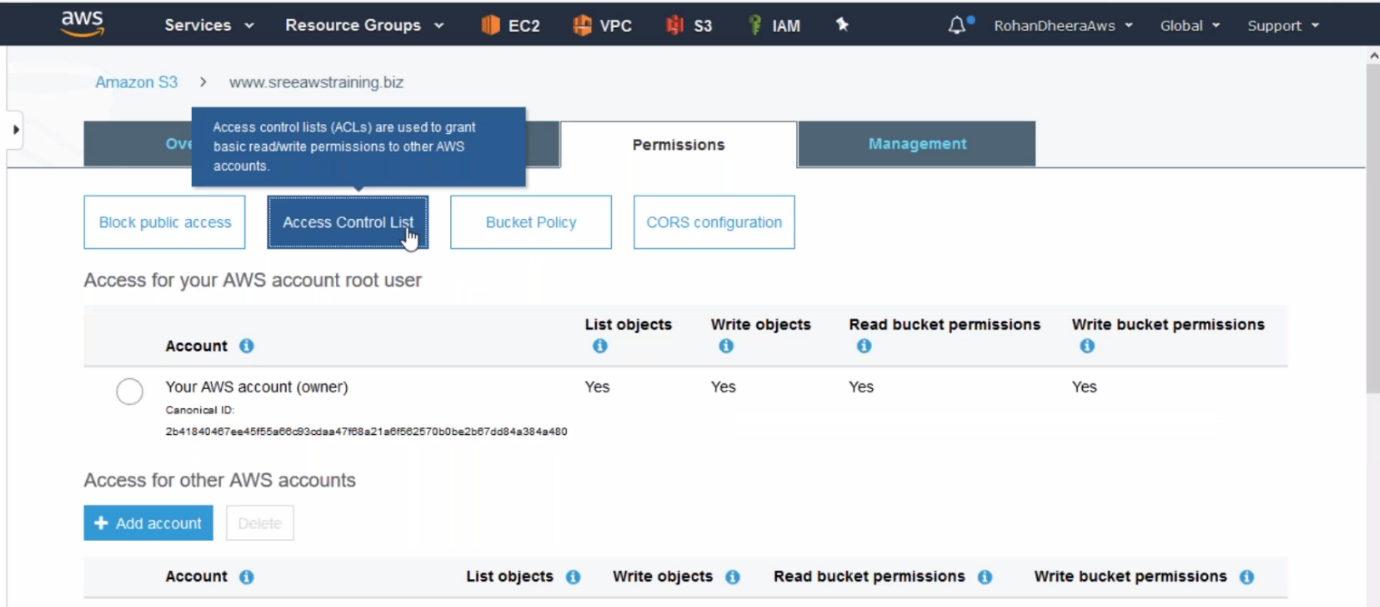


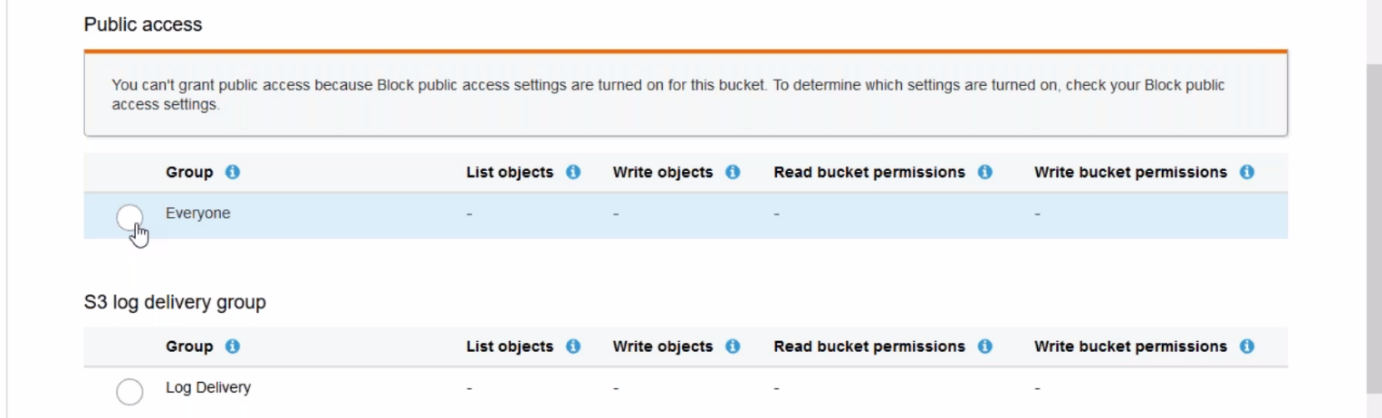
--- there is 2 ways we can access the content through internet 1.Access control list 2.Bucket Policy

**1.Access Control List**

Access Control List are used to grant basic read write permission to other AWS account or everyone or S3 log delivery group.

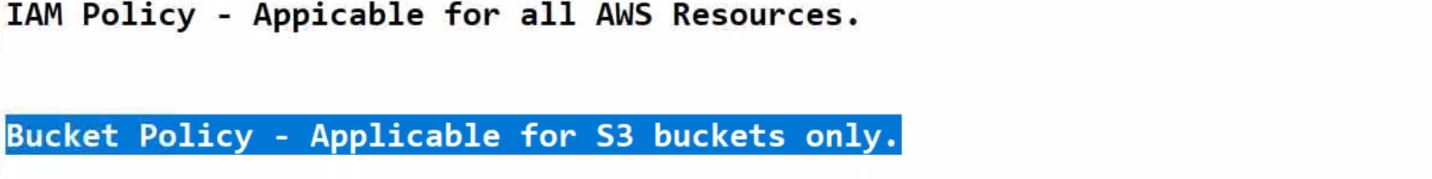
This feature don’t have granular control means if you want to give access to specific IP address, this type of specific options are not available in Access Control List





**Bucket Policy**

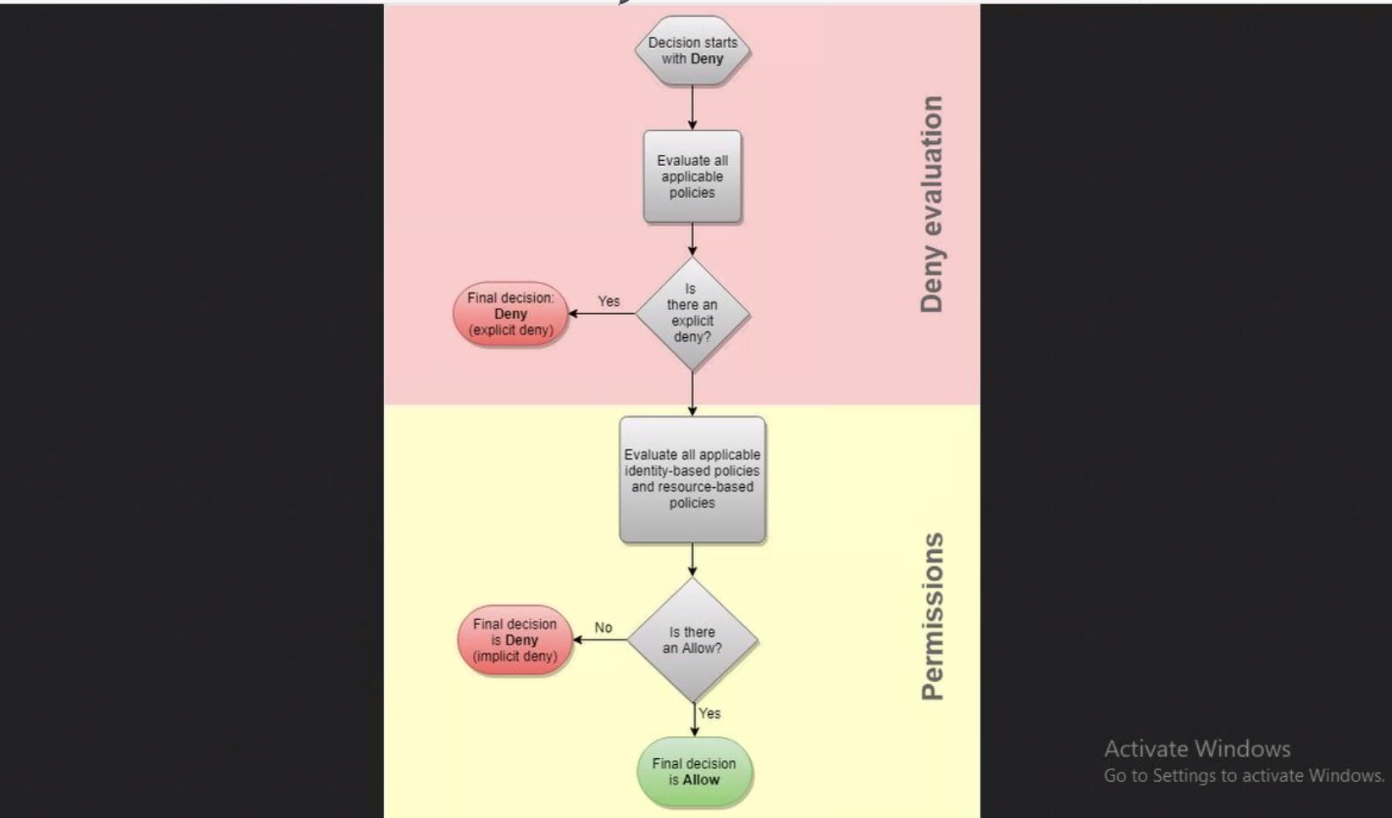
There are different policy are available in AWS, the major policies are 1.IAM policy 2. Bucket policy

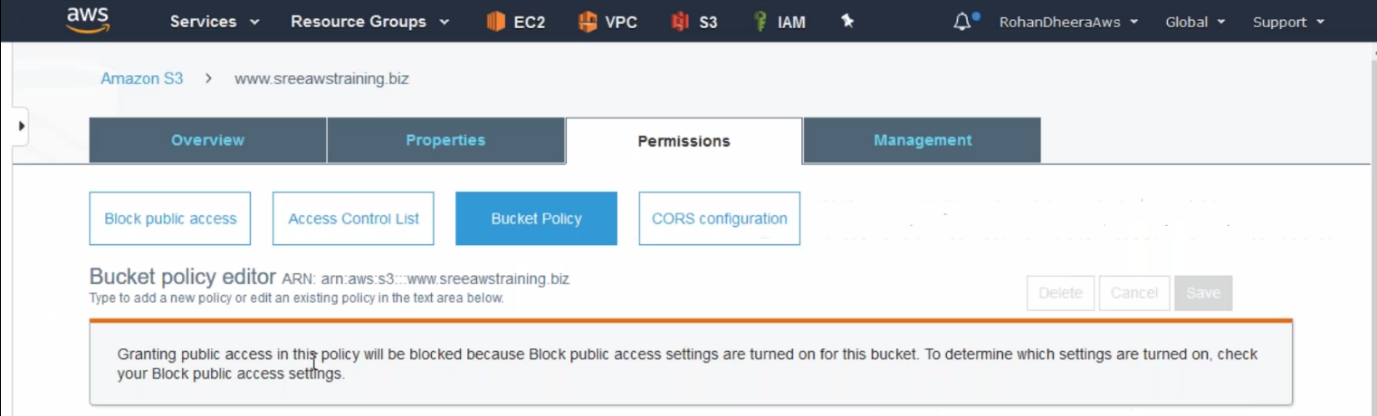


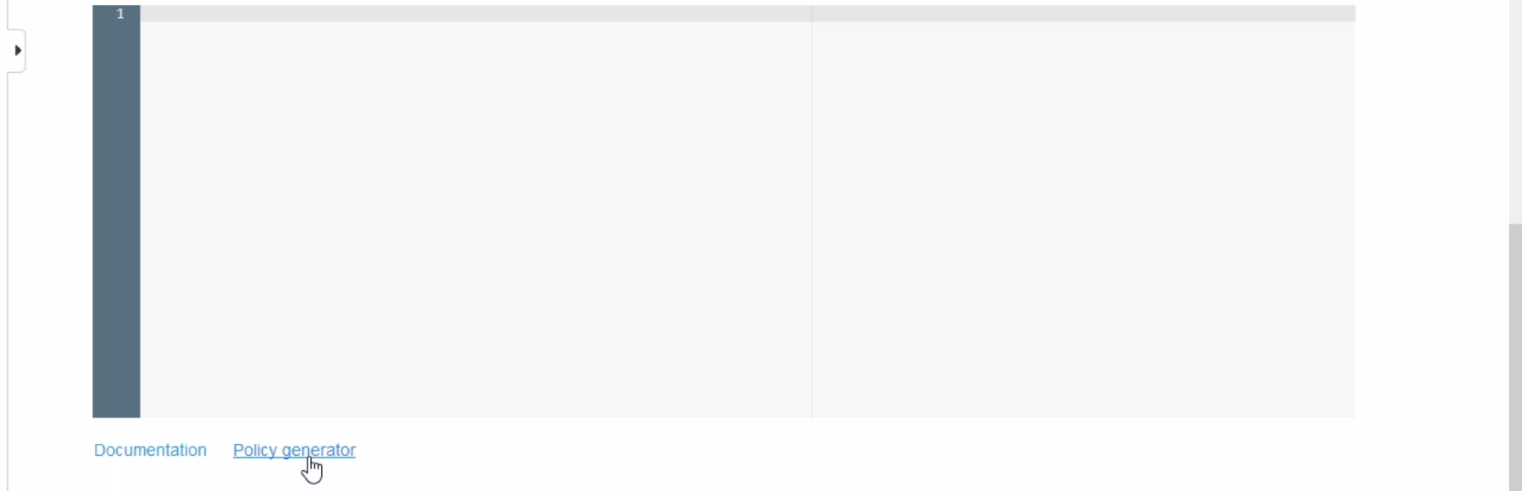
--- you want give permission to specific users then use IAM policy.

--- you want give permission to all user’s or world then use Bucket policy.

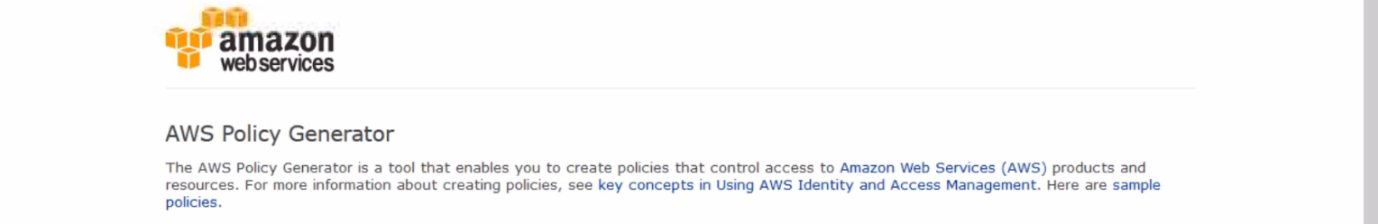
**AWS bucket policy evolution**

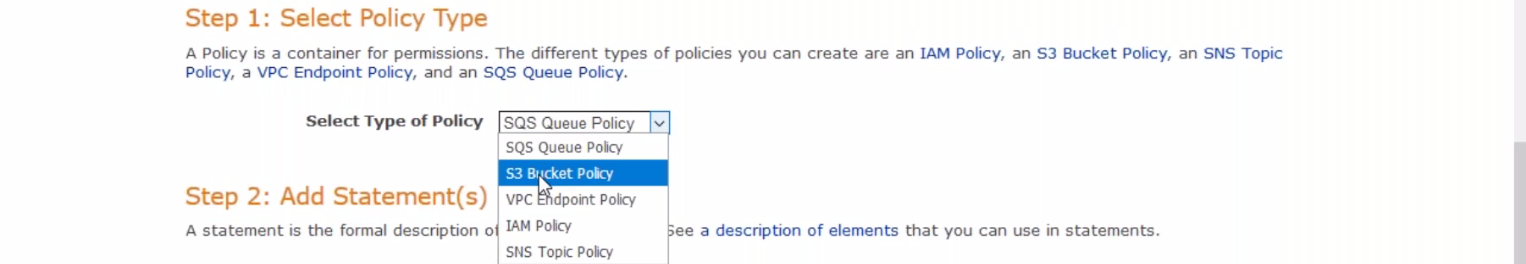






--- you want to generate new policy click on Policy generator.

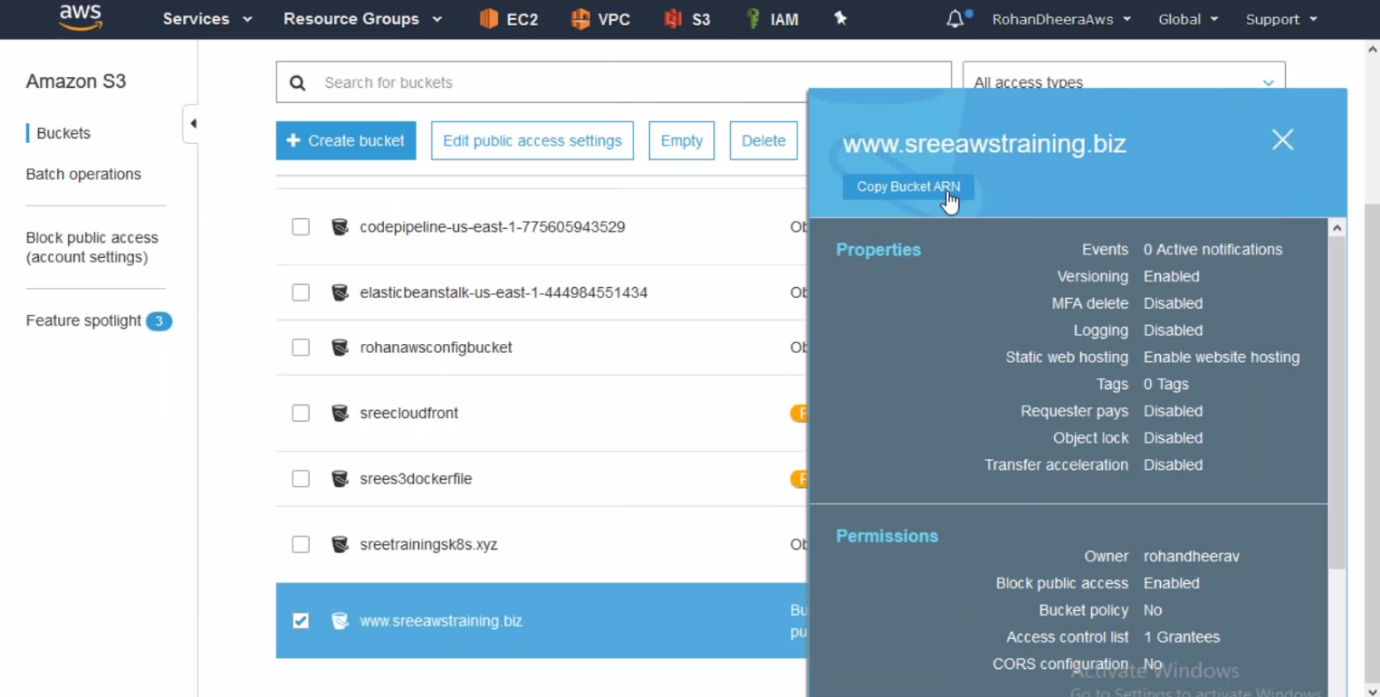






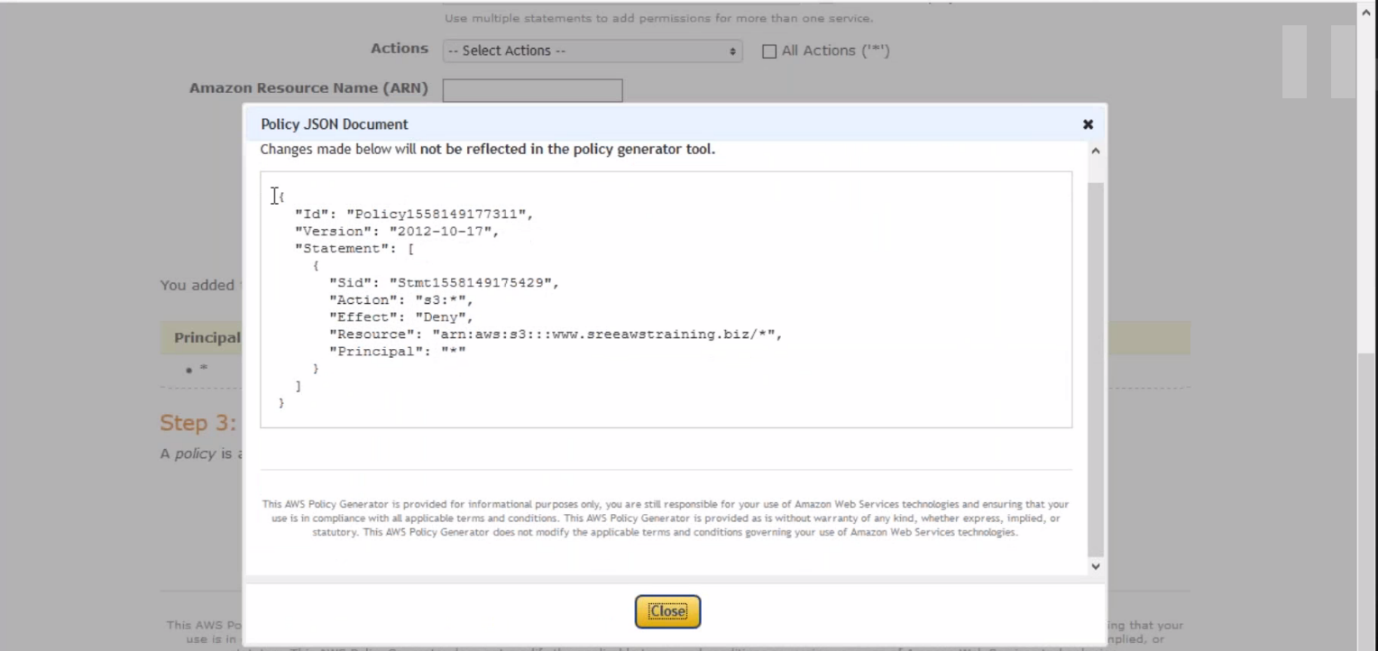


--- you will find the ARN here and next click on add statement





--- click on generate policy



--- copy the policy and paste it on BUCKET POLICY.

--- granular level permission like certain ip address access or account access…etc that is why we don’t use ACL(access control list). We are still using bucket policy

--- we can access the s3 bucket by using specific ip address

{

"Id":"PolicyId2",

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

"Statement":[

{

"Sid":"AllowIPmix",

"Effect":"Allow",

"Principal":"\*",

"Action":"s3:\*",

"Resource":"arn:aws:s3:::prabhu9652/\*",

"Condition": {

"IpAddress": {

"aws:SourceIp": [

"54.240.143.0/32",

"54.240.144.0/32"

]

}

}

}

]

}

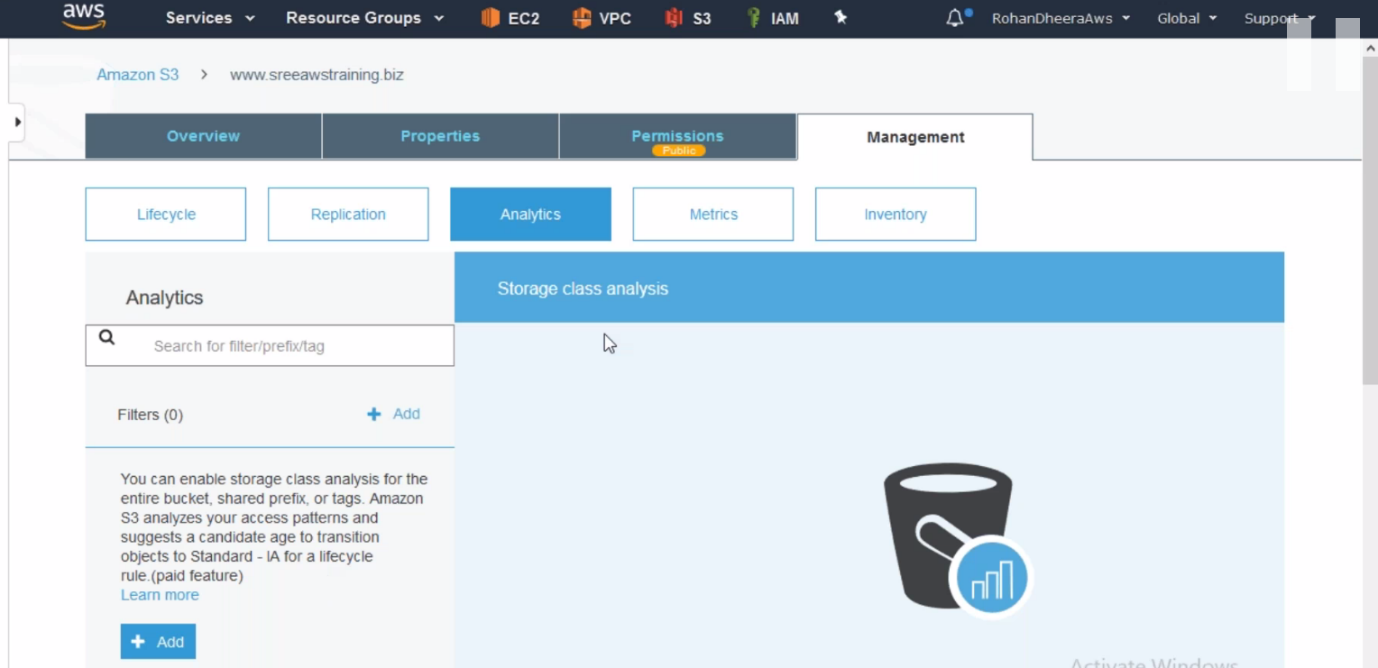
--- we are giving specific subnet ip address we have to add like this /32.

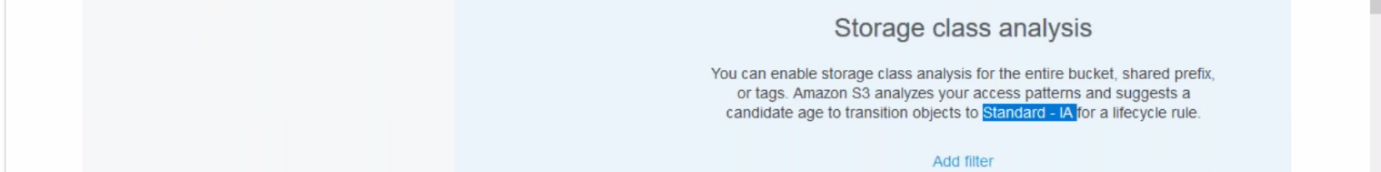
**MANAGEMENT**

In management there are 5 components and among the 5 components 2 components are important.

1.Life cycle 2. replication remaining 3 are use full when you receiving tera bytes of data daily

**Analytics**

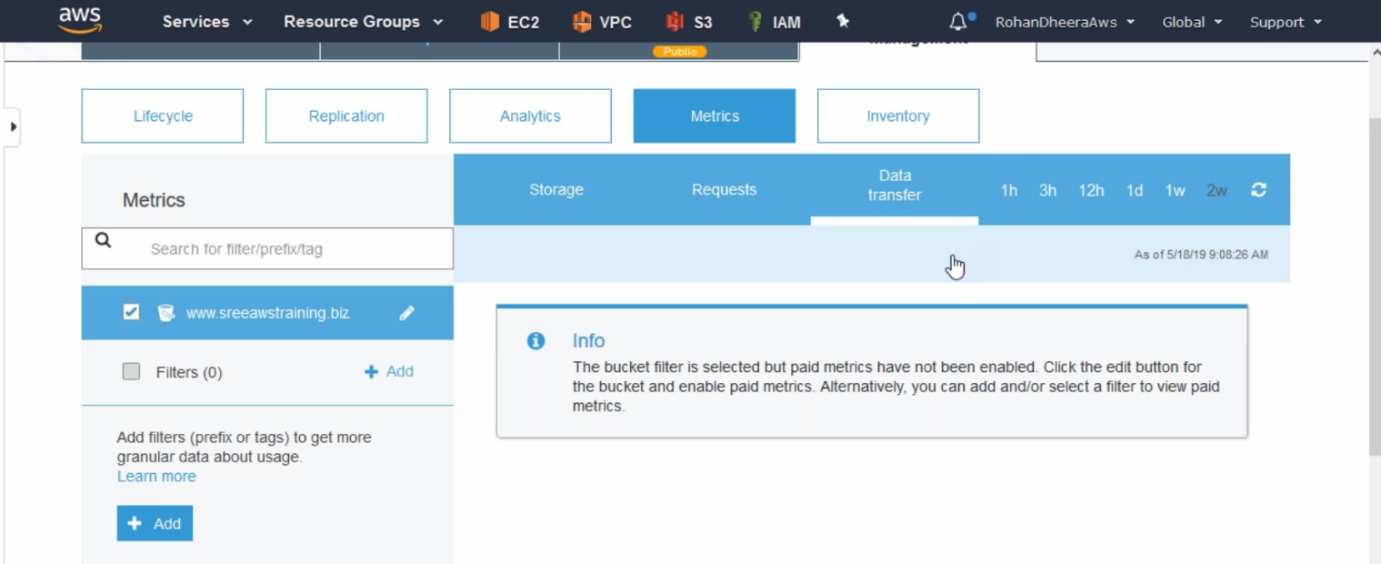




--- it is a paid feature.

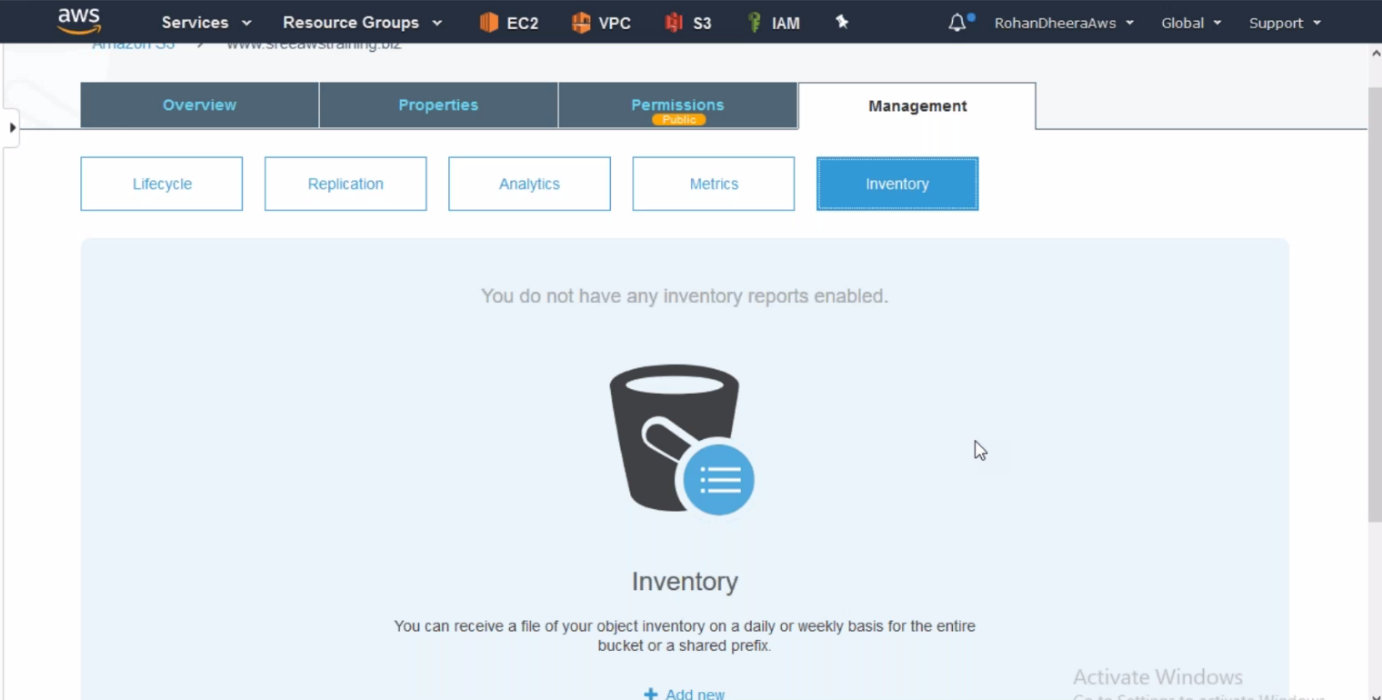
**Metrics**

How much data is being used and transferred?

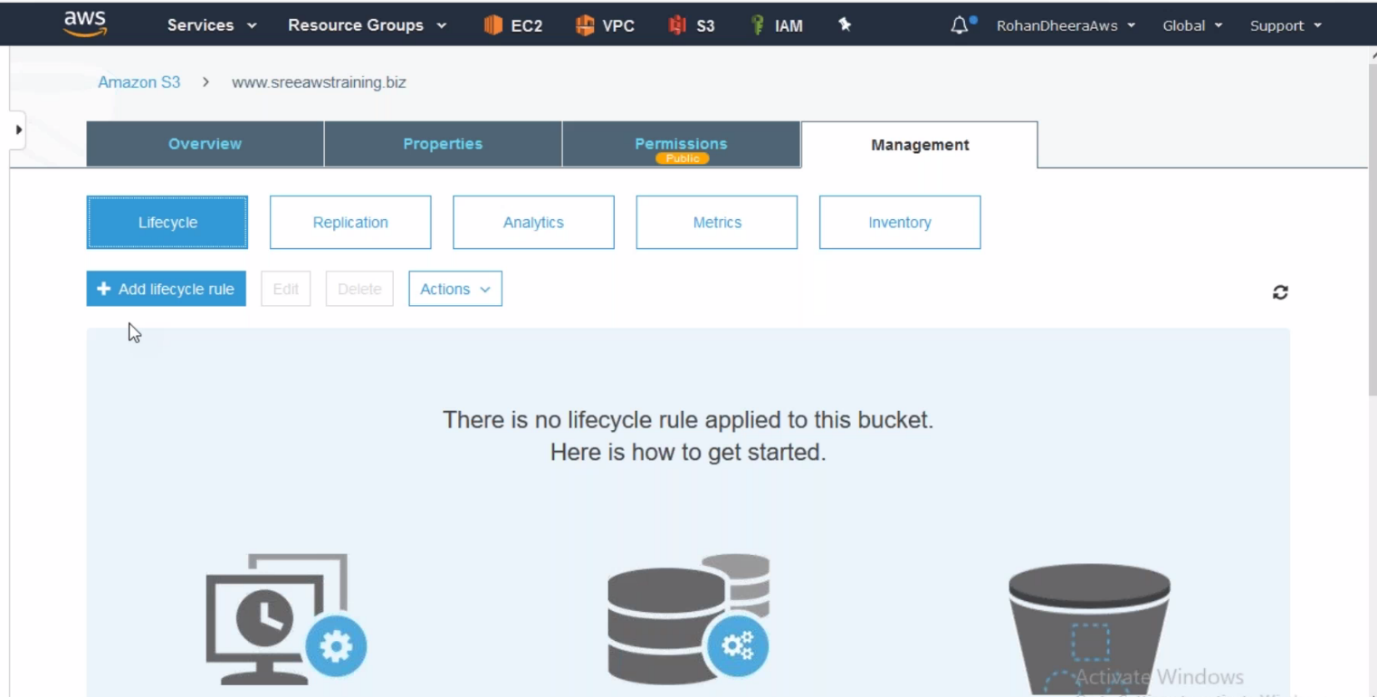


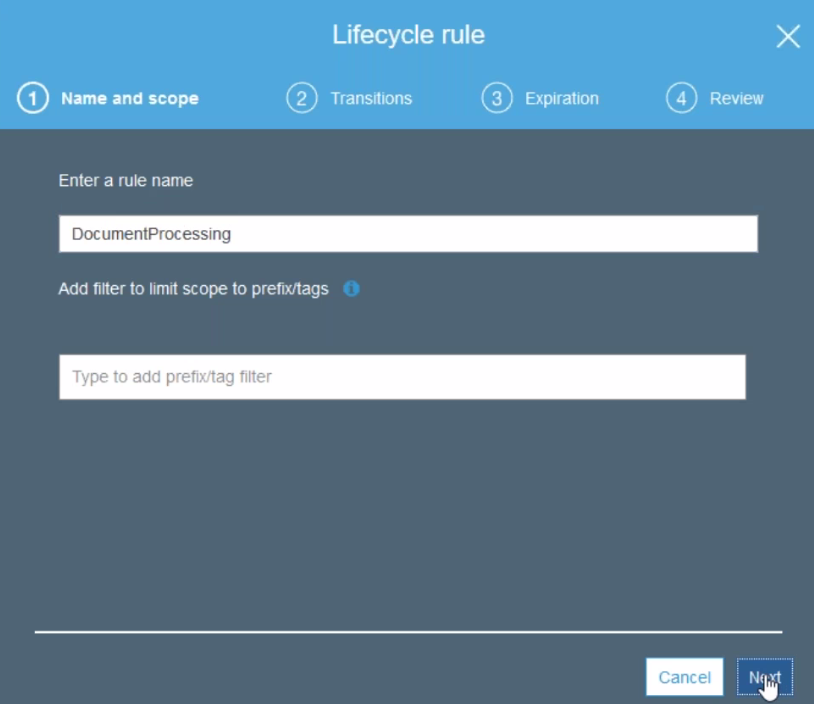
**Inventory**

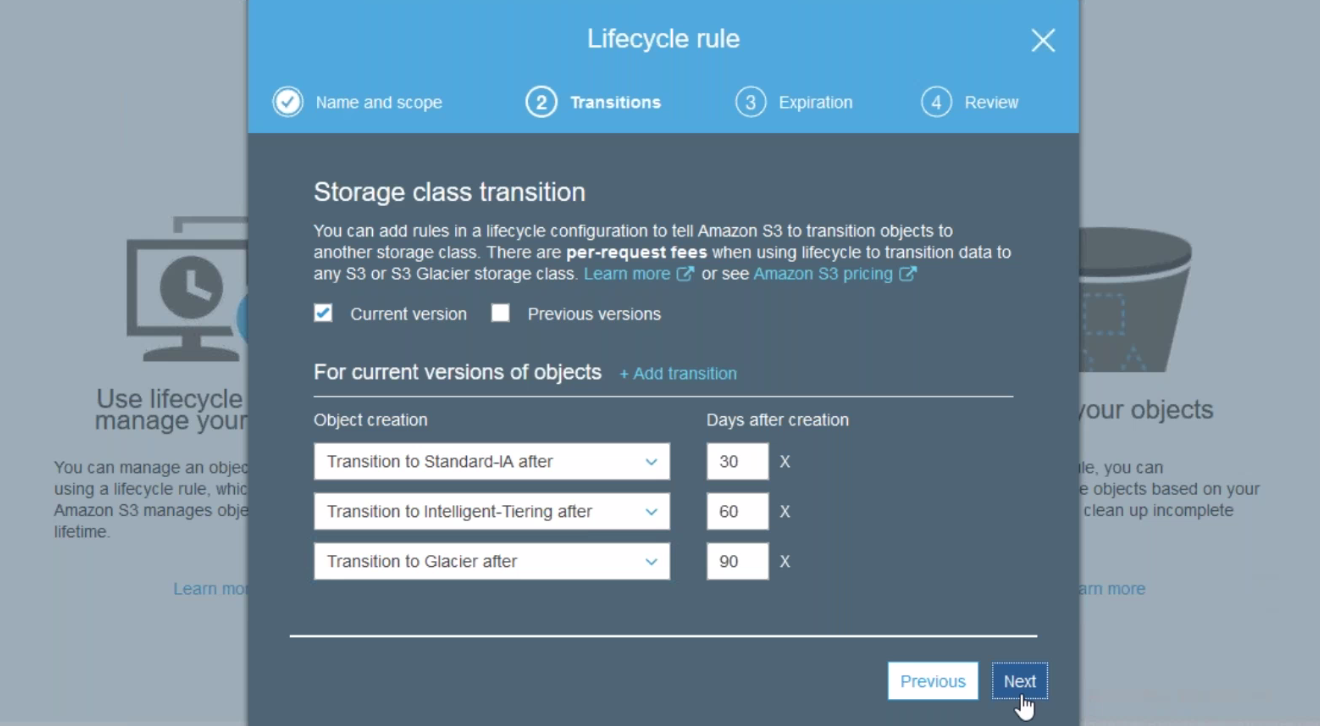
You want to know type of files are uploaded to your AWS S3 from user then use this feature.



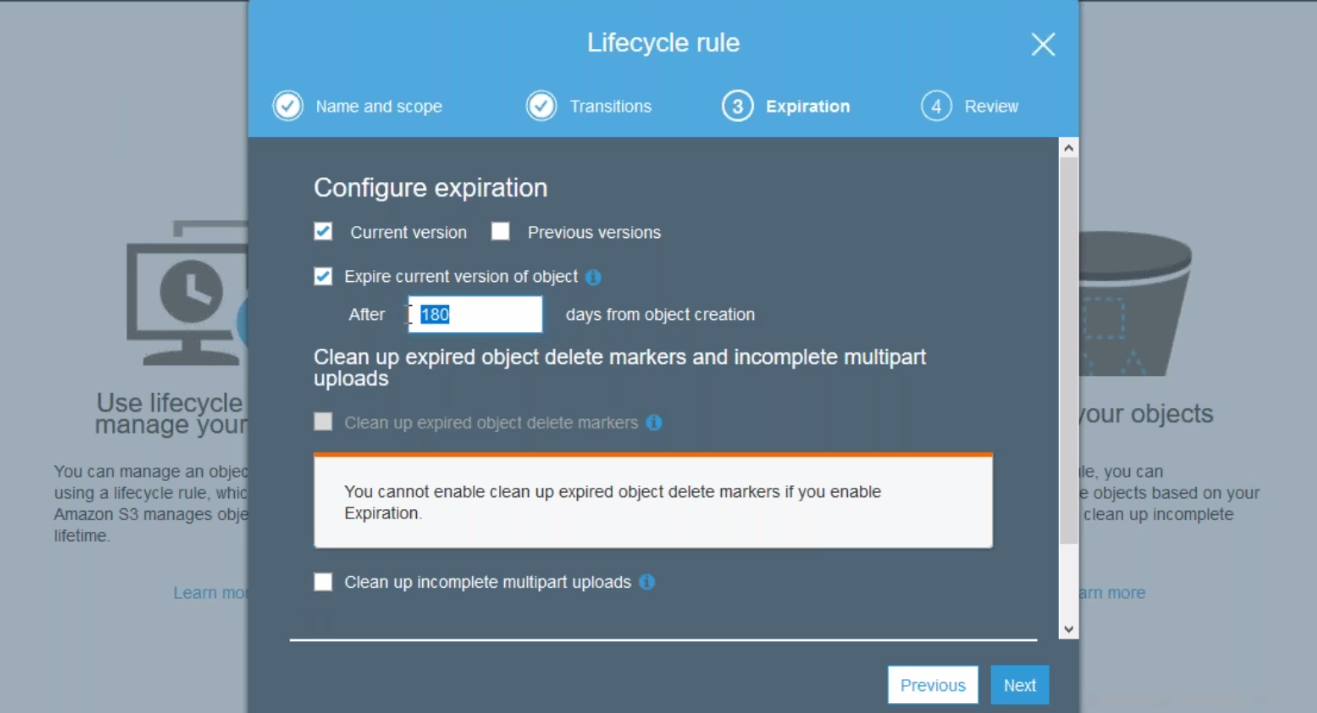
**Life cycle**



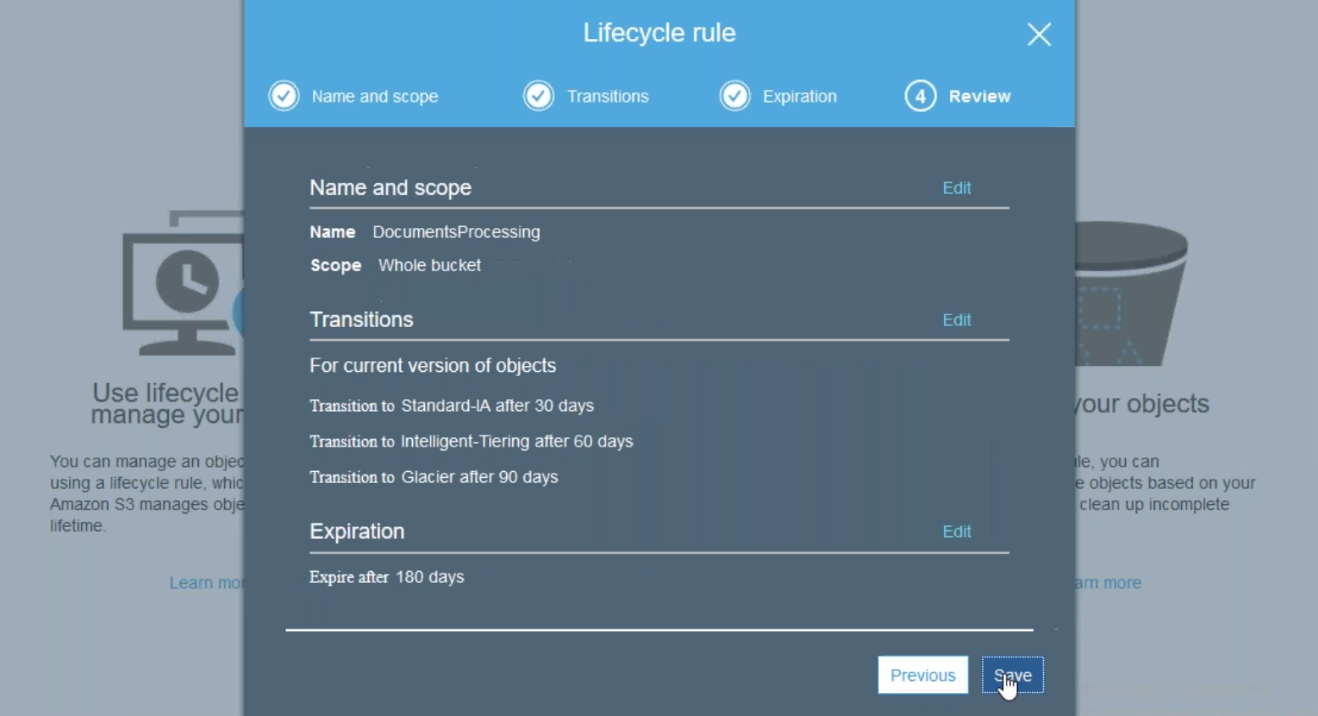




--- if you upload a file to S3 1st it moved to standard then after 30days it moved to IA

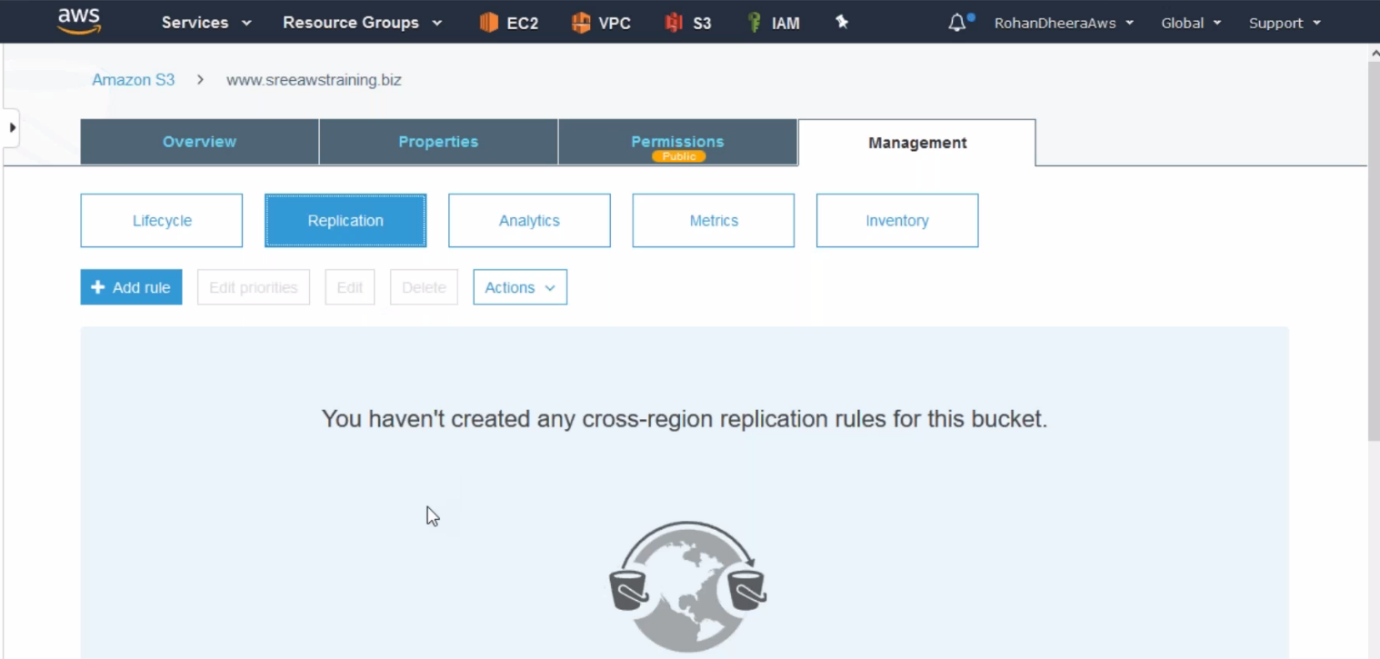


--- after 180 days the file will be expired. You can give also yrs also.

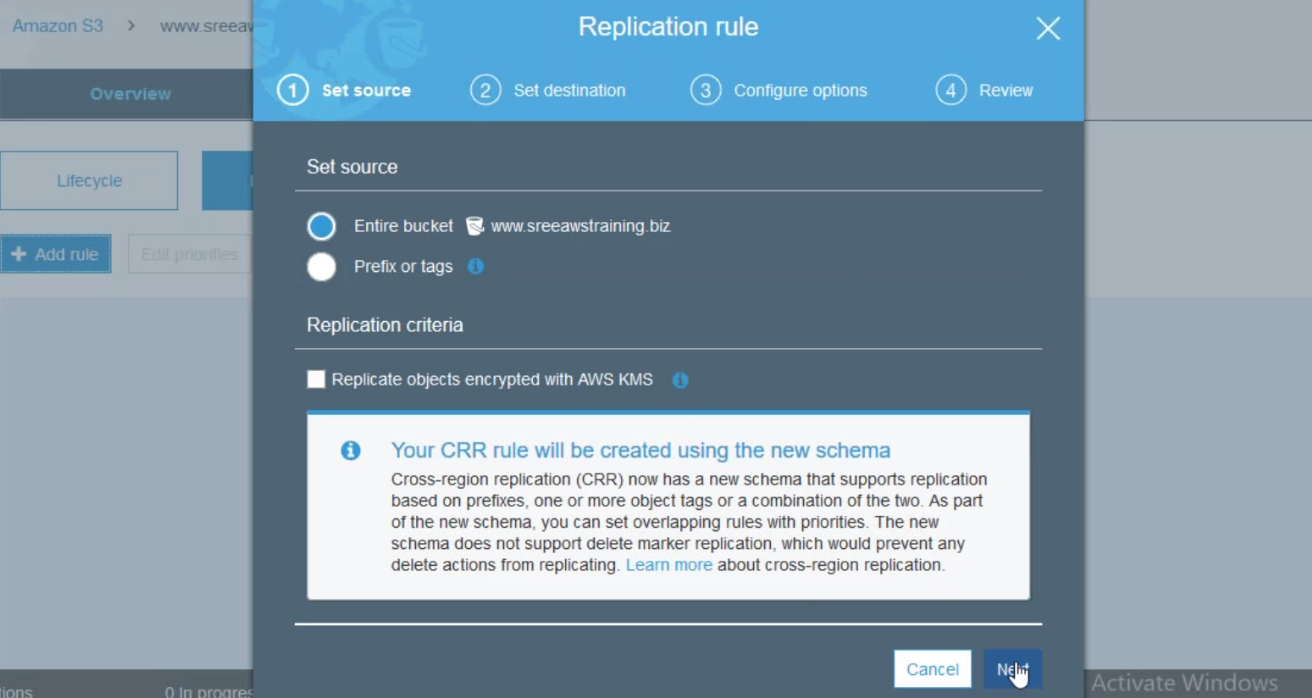


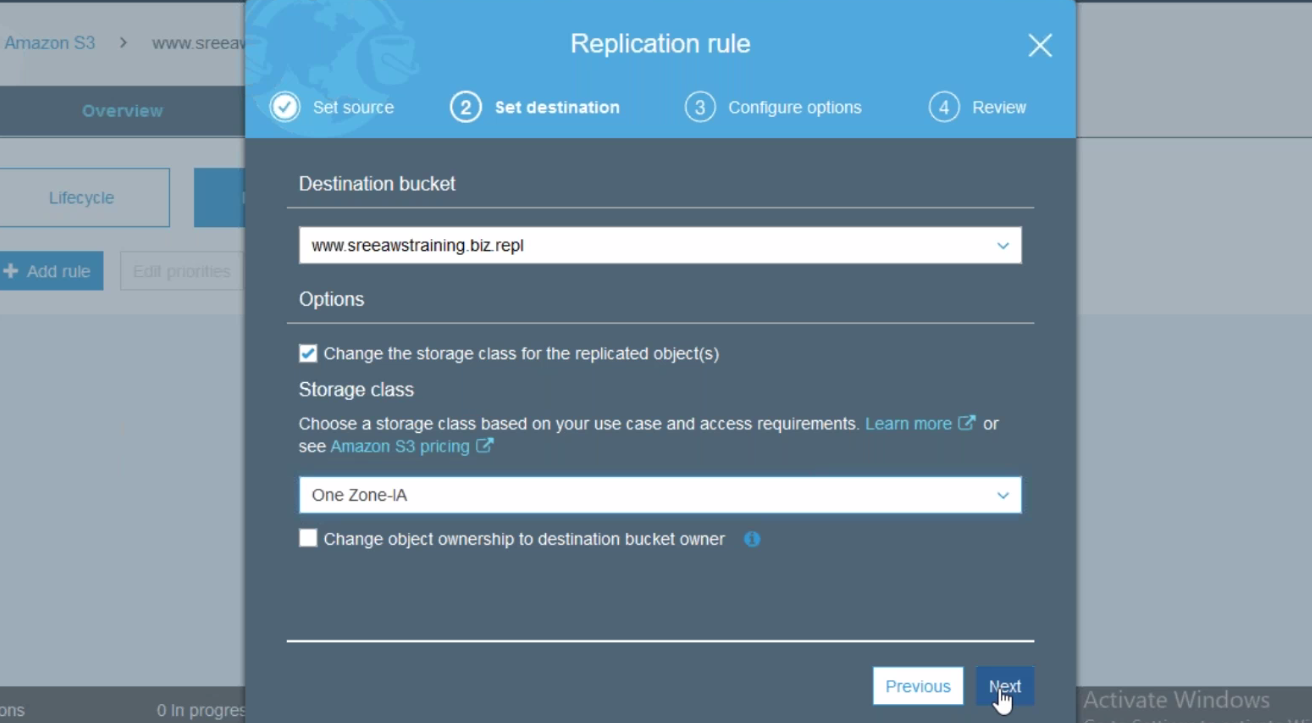
--- the life cycle will be saved.

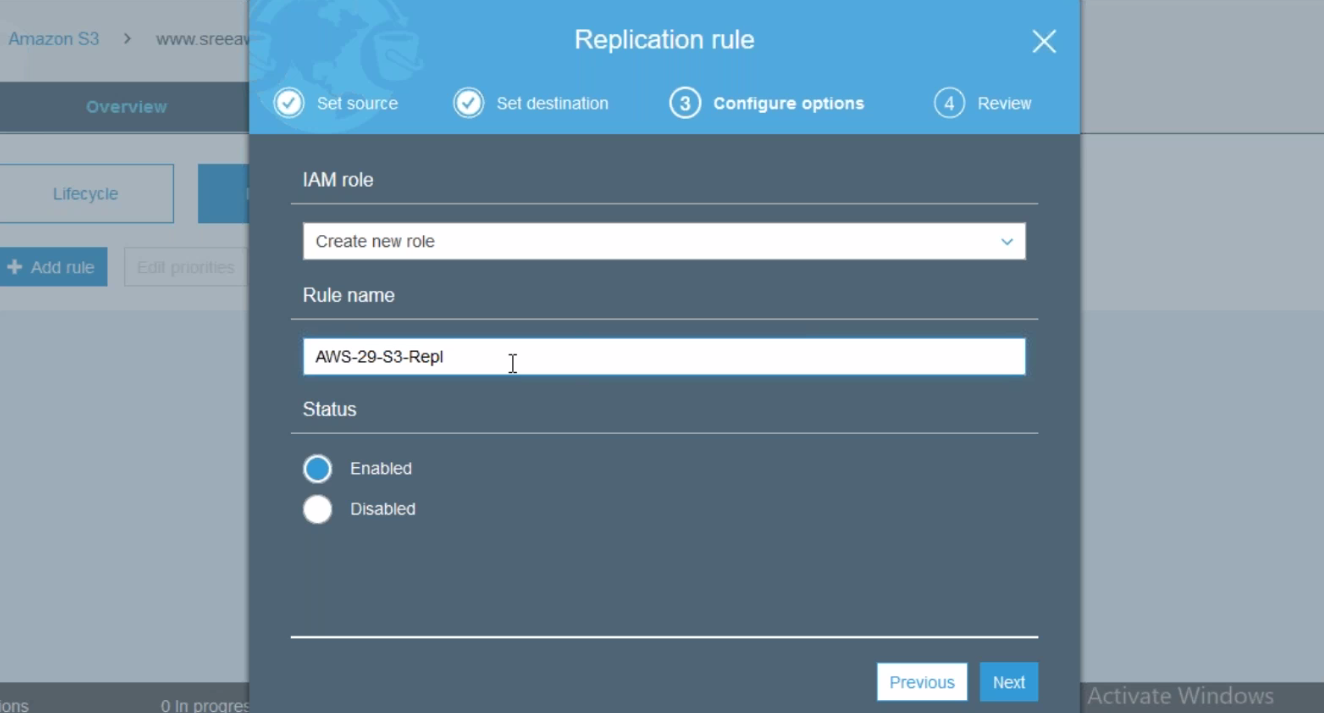
**Replication**   
 you want to replicate the data from one bucket to another bucket. Replication works with availability zones not with different location and you need to enable the replication before uploading the data.

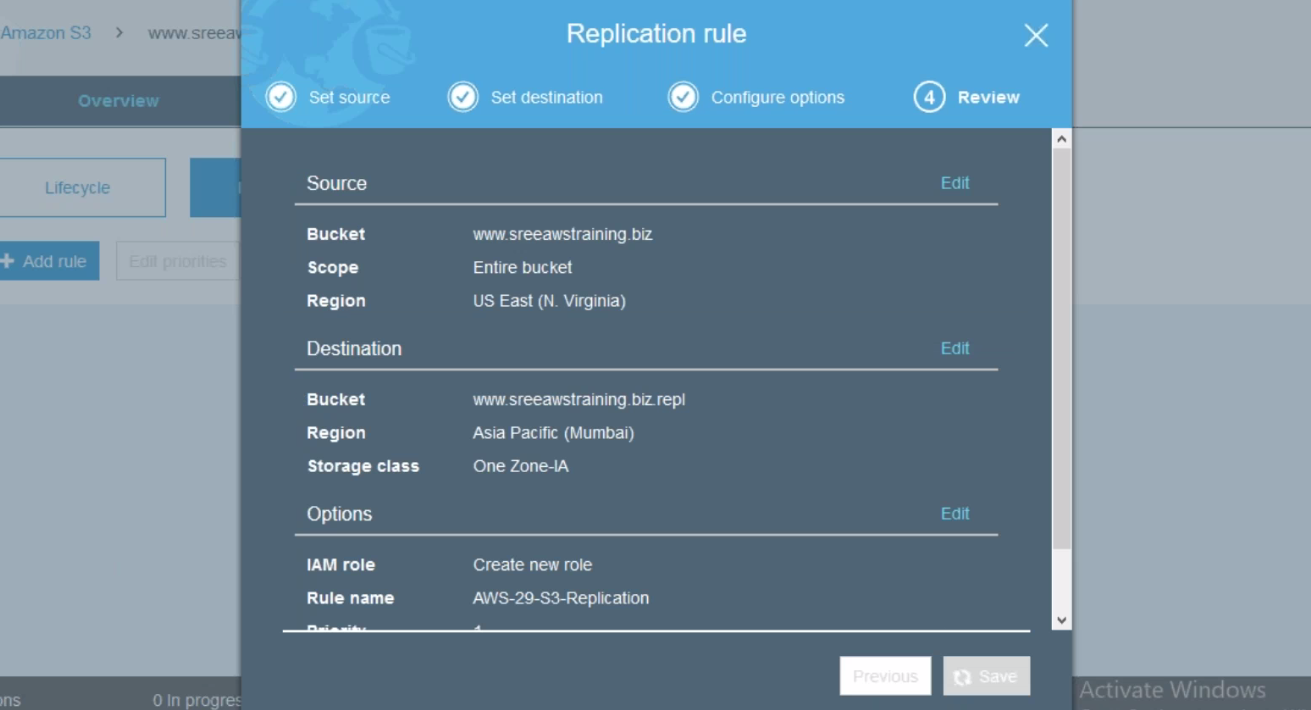












--- now you upload any data it will be replicated to destination bucket you mentioned in the life cycle.

**--- QUES Difference between sync and a-sync …?**

Imagine we have 2 servers and one client, we sync the data from the client, 1st the data copied to the server-1 and then the data copied to the server-2, if the one server goes down then the data will available from the other server then the confirmation is done. In the case of a-sync the data from the client is coped to the server-1, the confirmation will be done, later the data from the server-1 copied to the server-2.