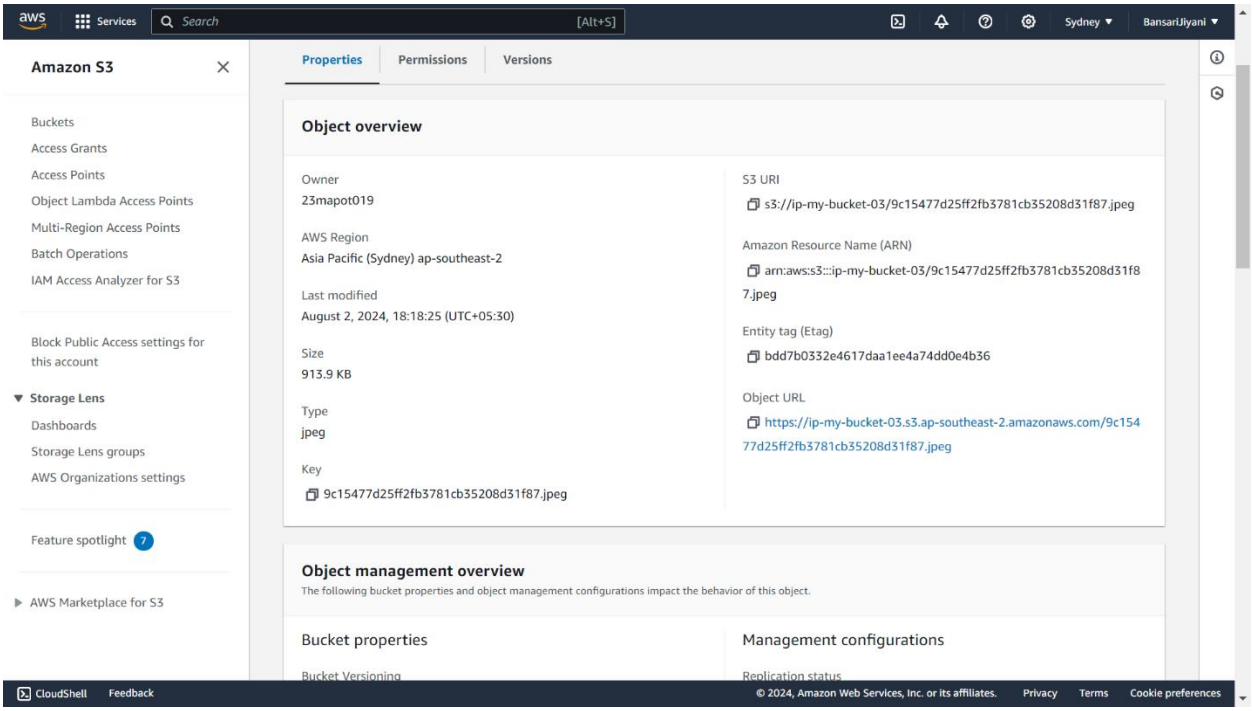
AWS S3

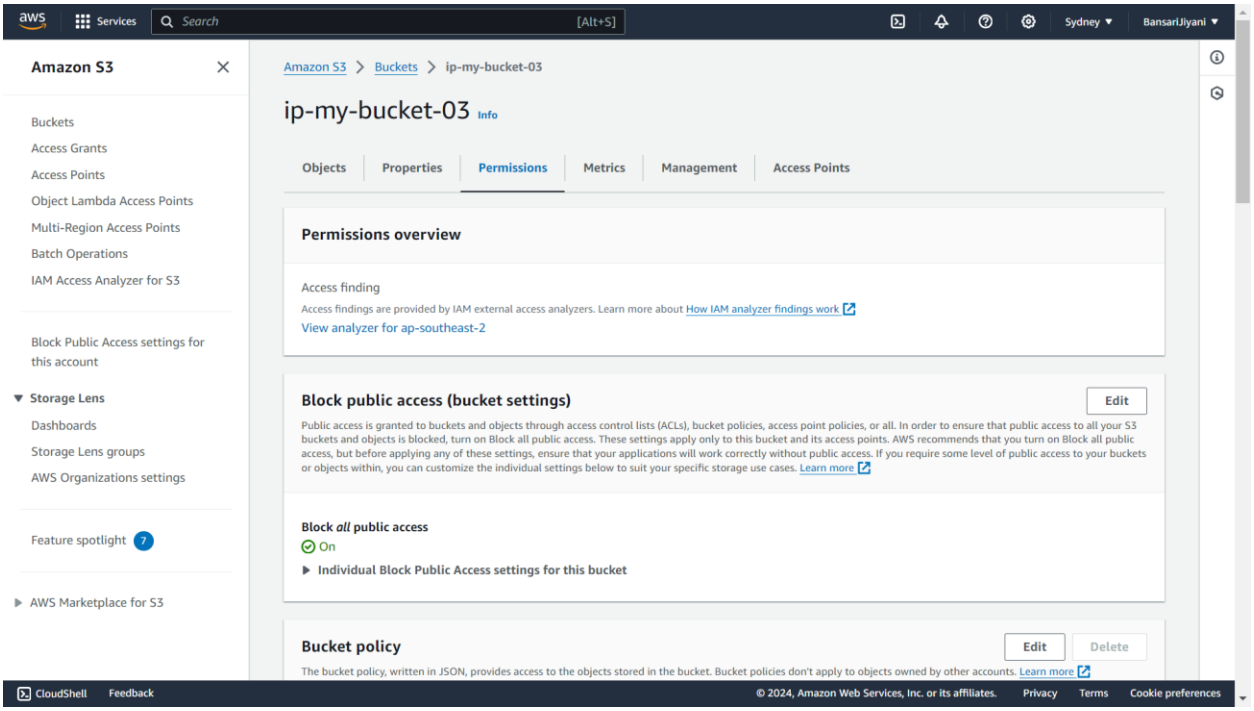
- **How to Make Private object URL to Public URL and Give Permission**

- **Storage Classes**

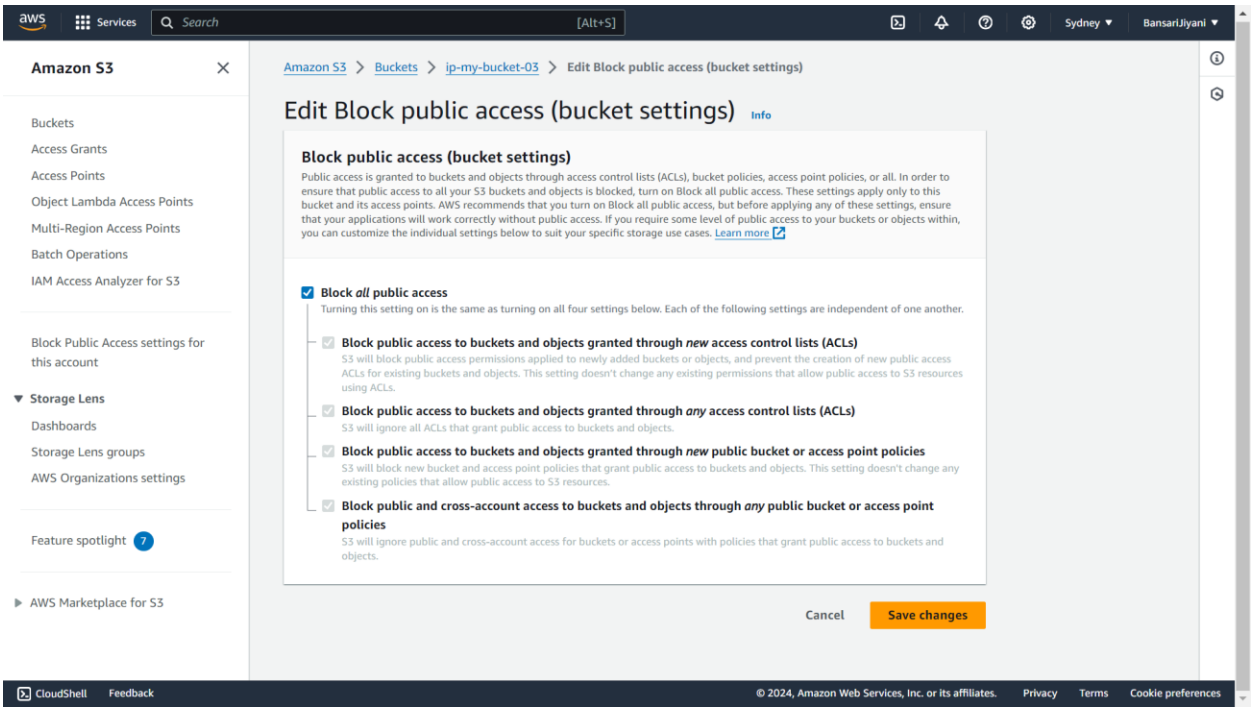
1. **Create Bucket and put some file or images or code and go to the properties of this object and Copy this Object URL and Paste In other page and when we try to access it then it Gives Error.**

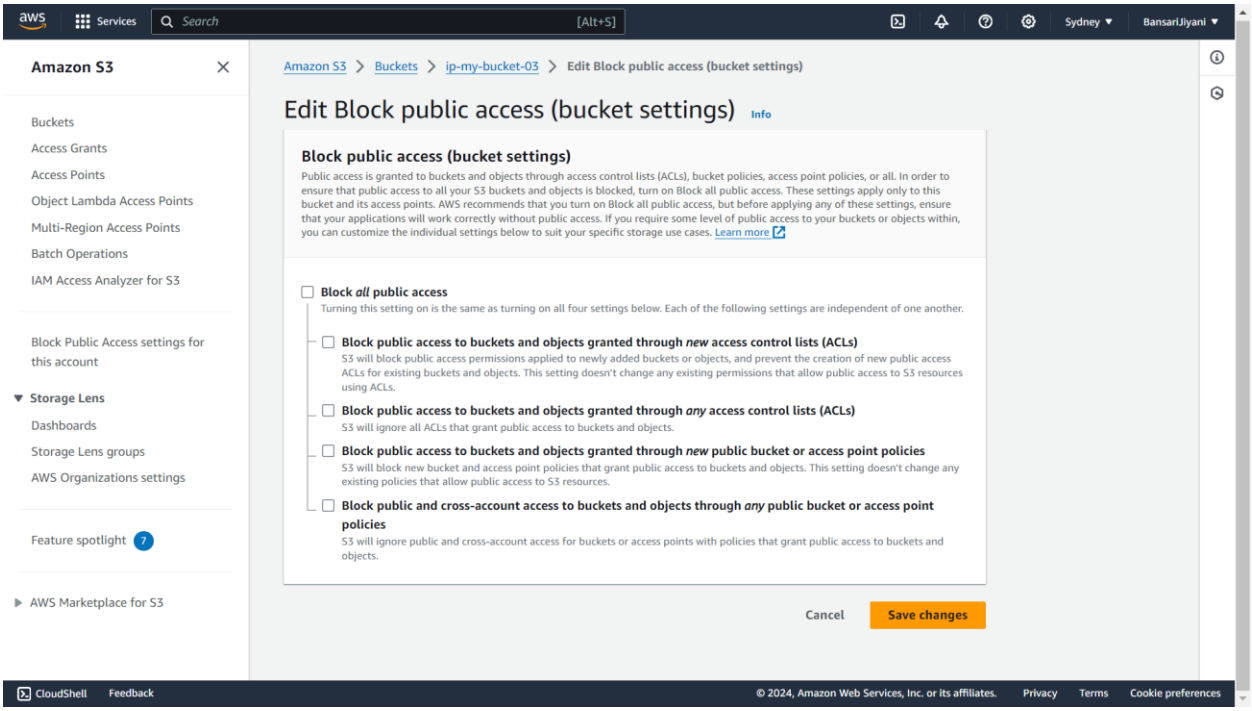


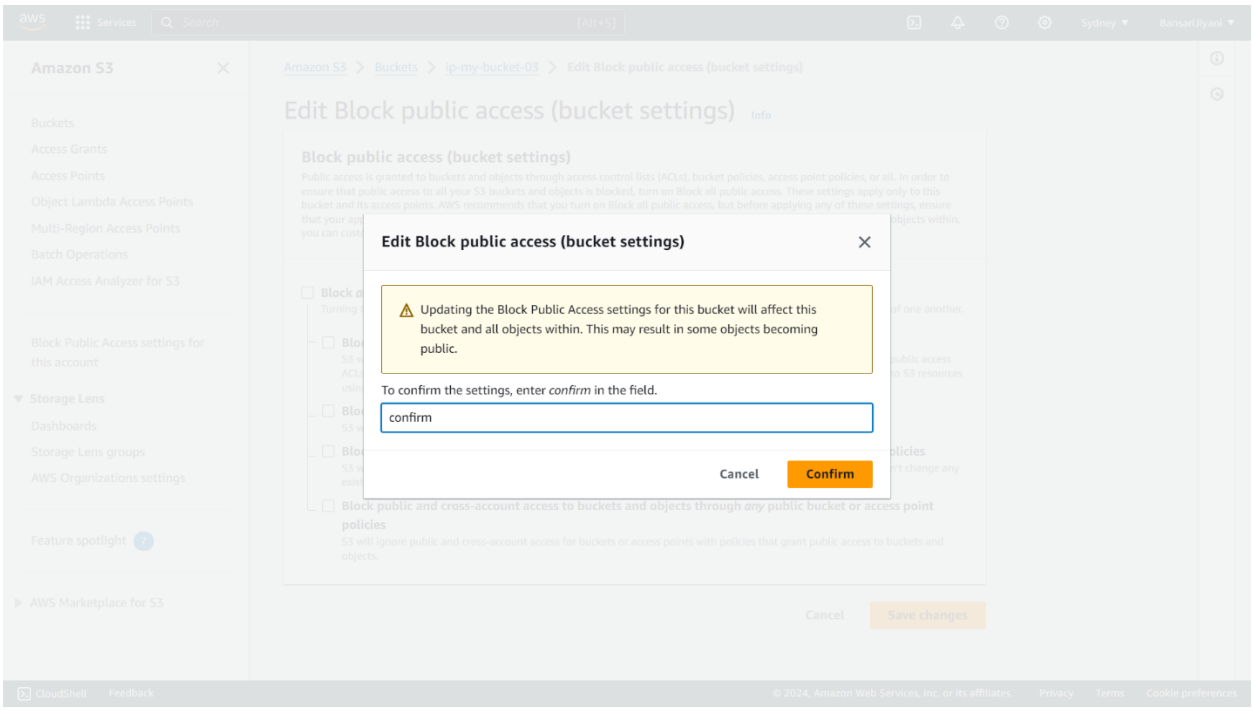
2. **Go to the permission of the bucket and edit the Block Public Access.**

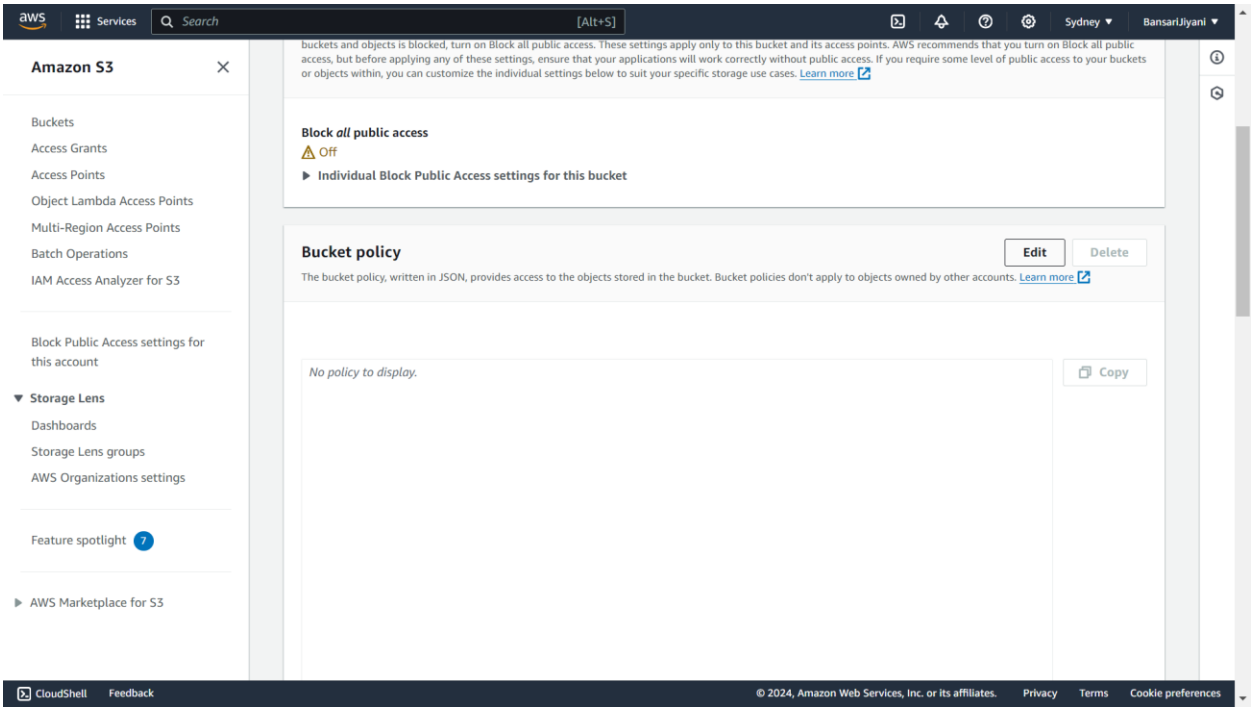


3. **Untick the Block all Public Access and Save changes and check Block All public Changes Will Off.**

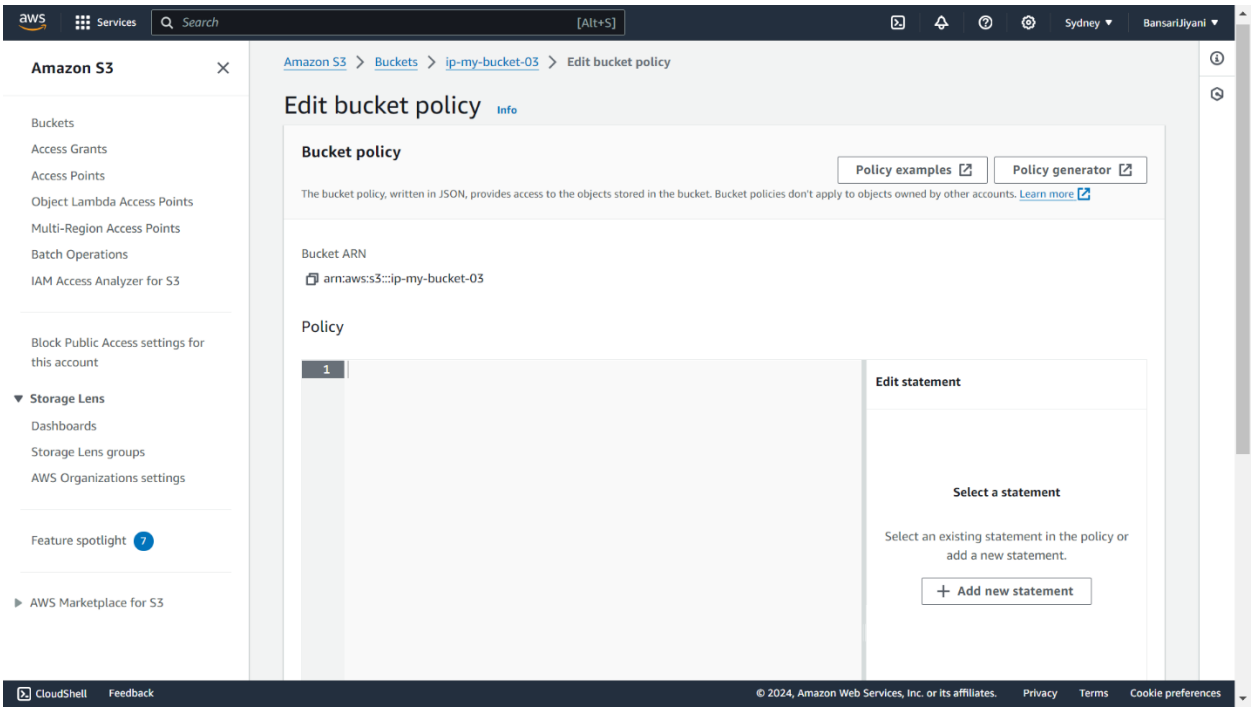

aws
Services
Search
[Alt+S]
Sydney
BansariJiyani
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets > ip-my-bucket-03 > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Cancel
Save changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
Sydney
BansariJiyani
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
AWS Marketplace for S3
Amazon S3 > Buckets > ip-my-bucket-03 > Edit Block public access (bucket settings)
Edit Block public access (bucket settings) Info
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Cancel
Save changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

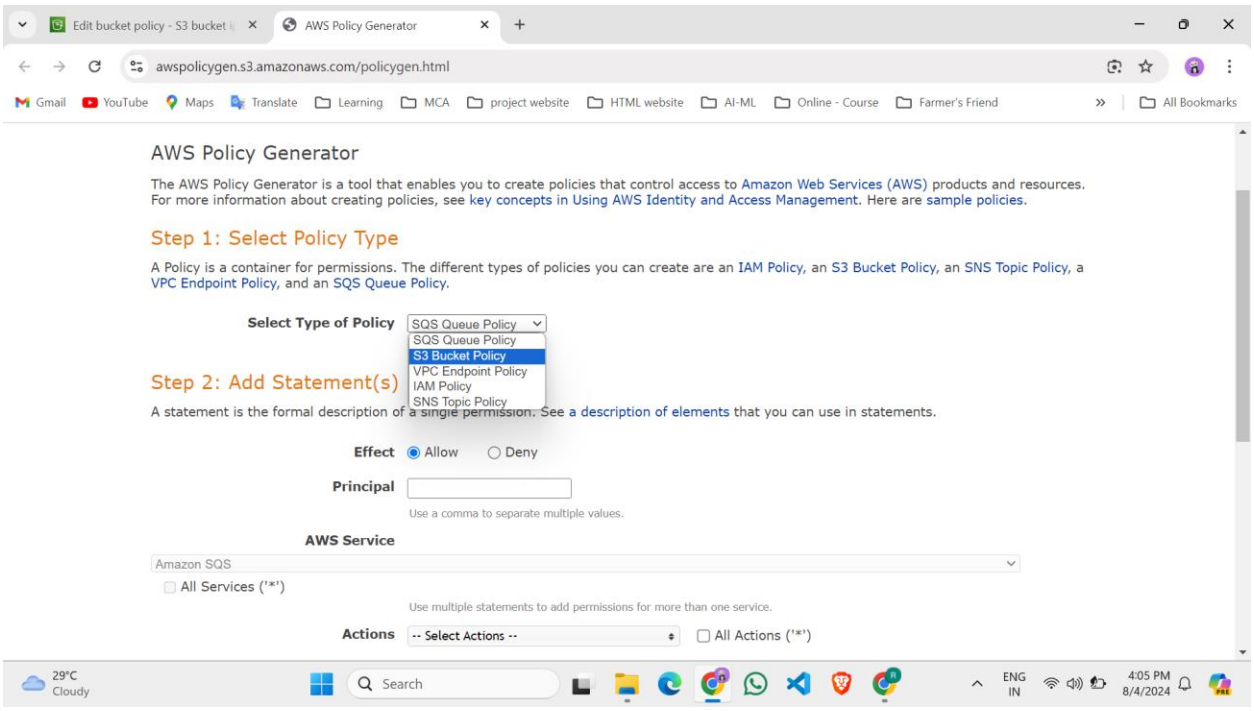


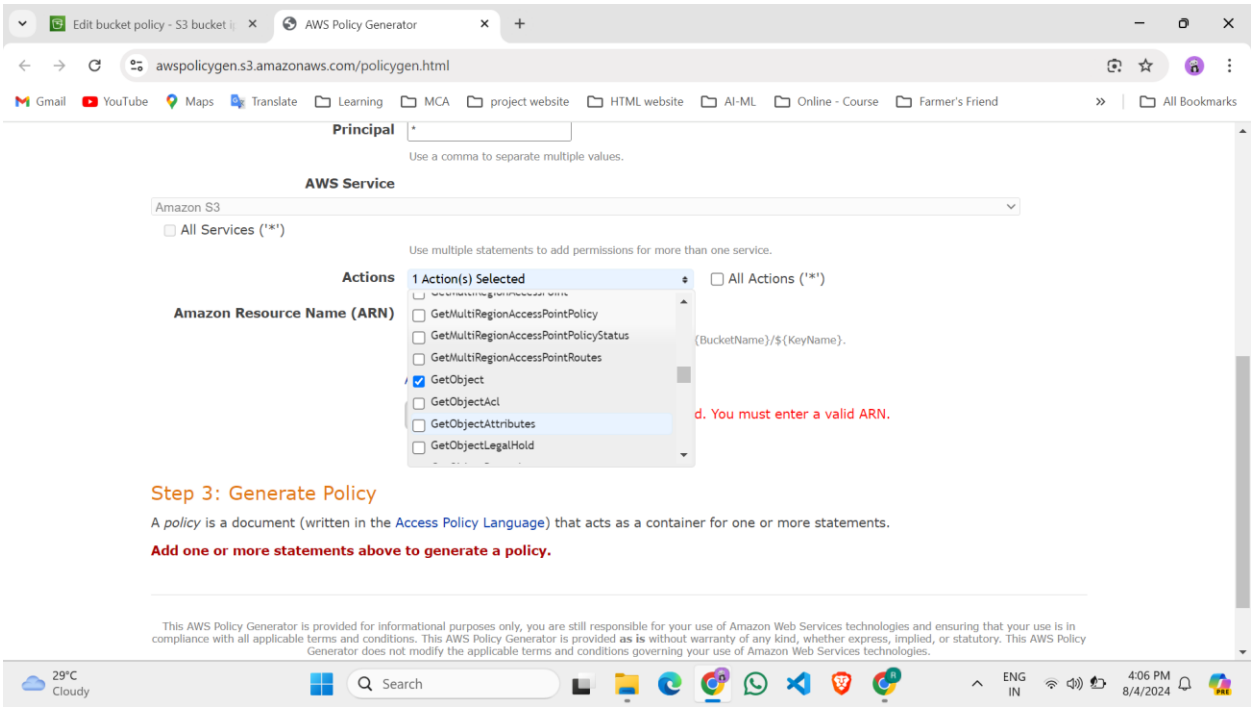


4. **Go to the Bucket Policy And edit it.**

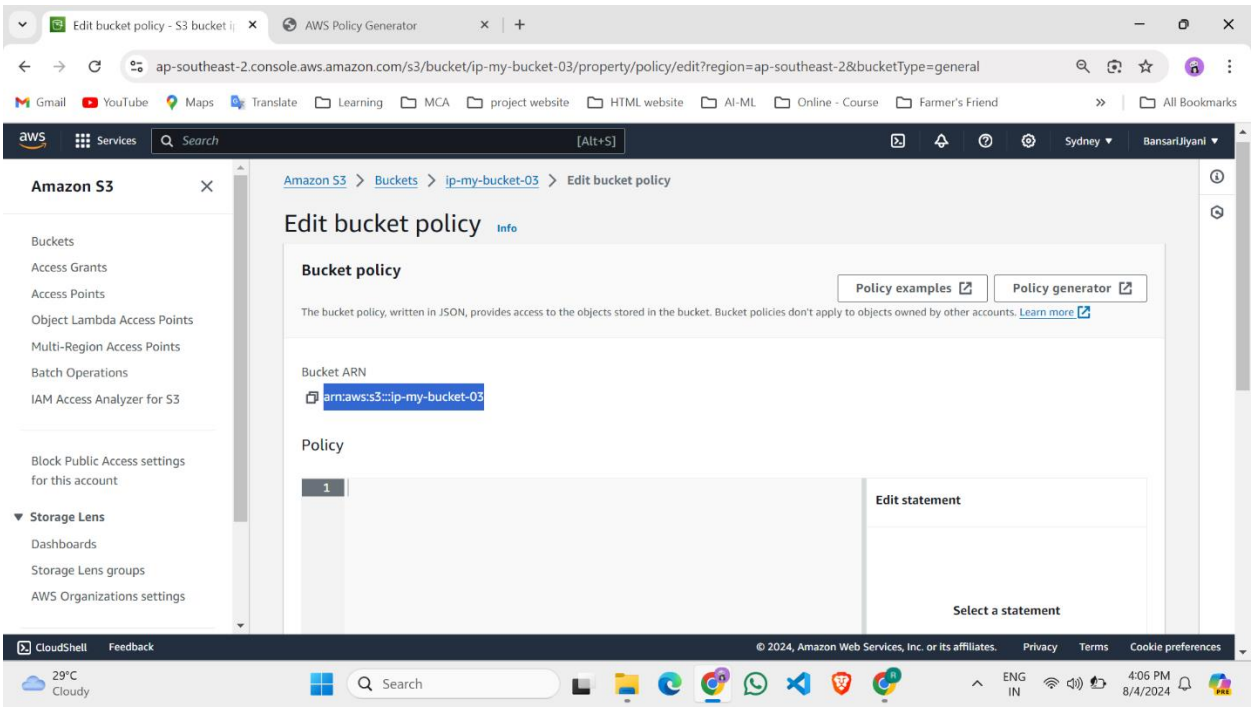


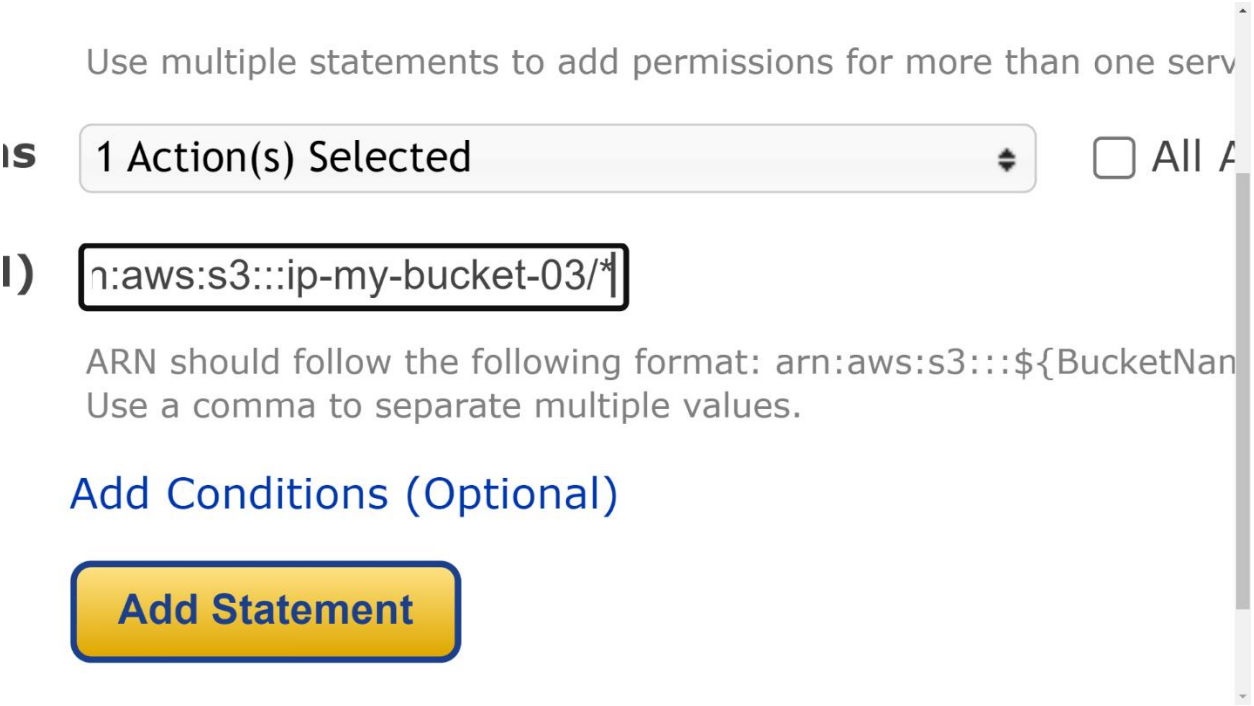
5. **Go to the policy Generator. and Select the S3 bucket in select type of policy.**
   In Effect select allow
   In principal Write * (* means all of can access this object)
   In Action Select GetObject

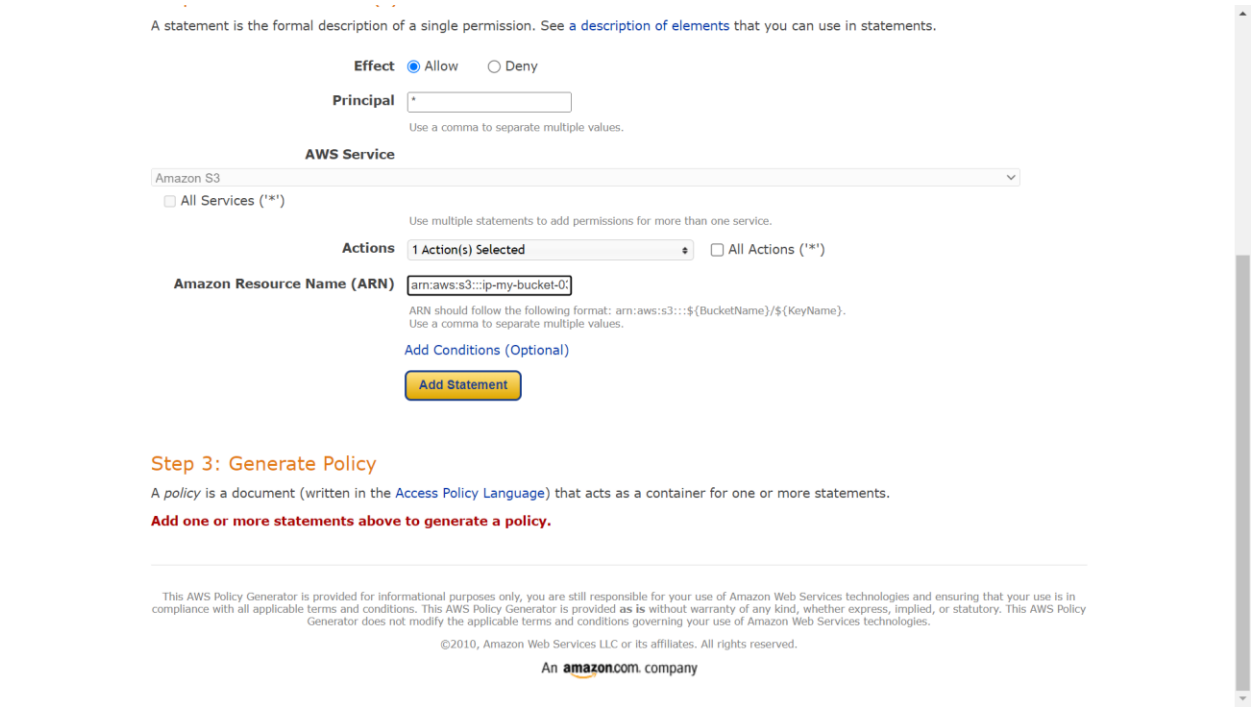




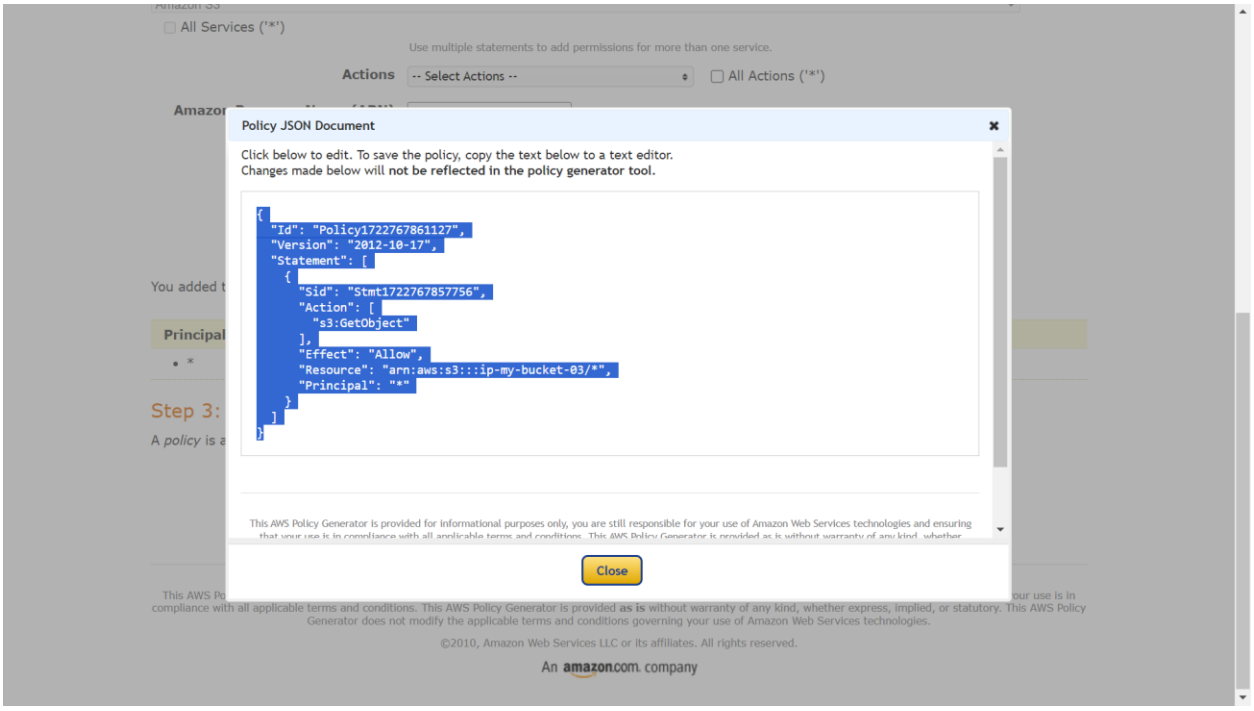
6. **Generate policy and Get ARN of bucket from the bucket policy and paste it in ARN and put /* after this ARN.**

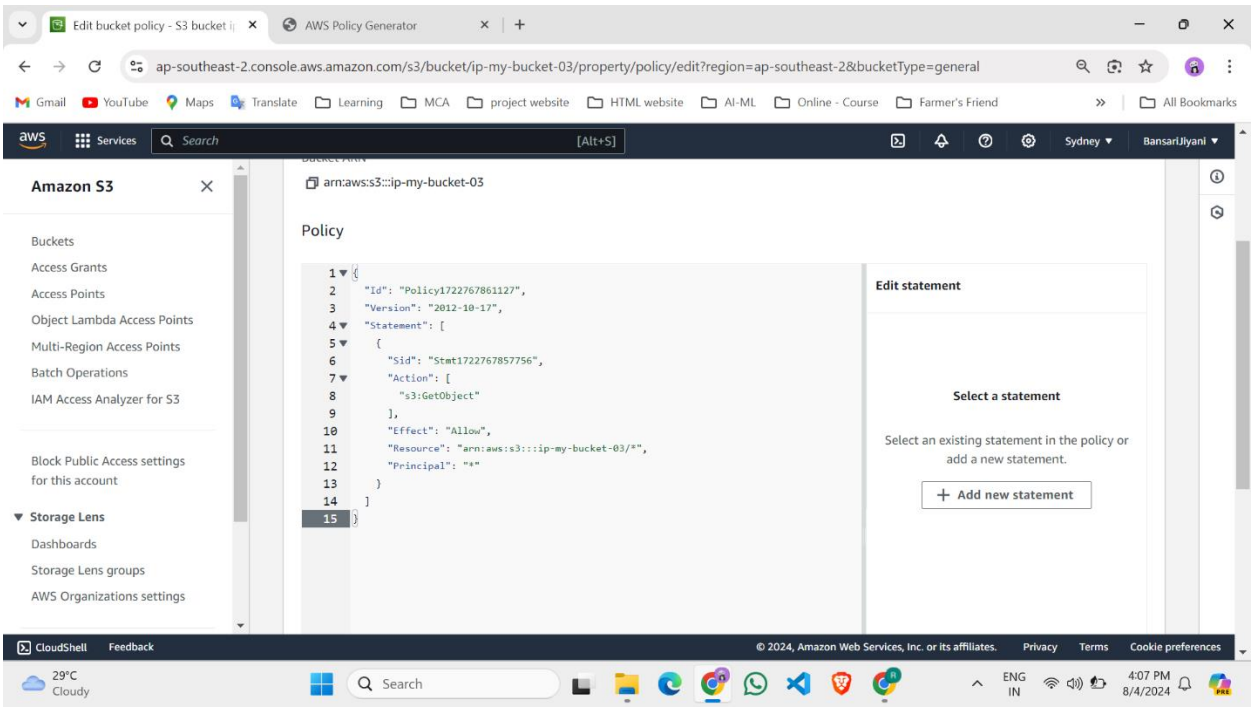

Edit bucket policy - S3 bucket
AWS Policy Generator
ap-southeast-2.console.aws.amazon.com/s3/bucket/ip-my-bucket-03/property/policy/edit?region=ap-southeast-2&bucketType=general
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Amazon S3 > Buckets > ip-my-bucket-03 > Edit bucket policy
Edit bucket policy
Info
Bucket policy
Policy examples
Policy generator
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Bucket ARN
arn:aws:s3:::ip-my-bucket-03
Policy
Edit statement
Select a statement
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

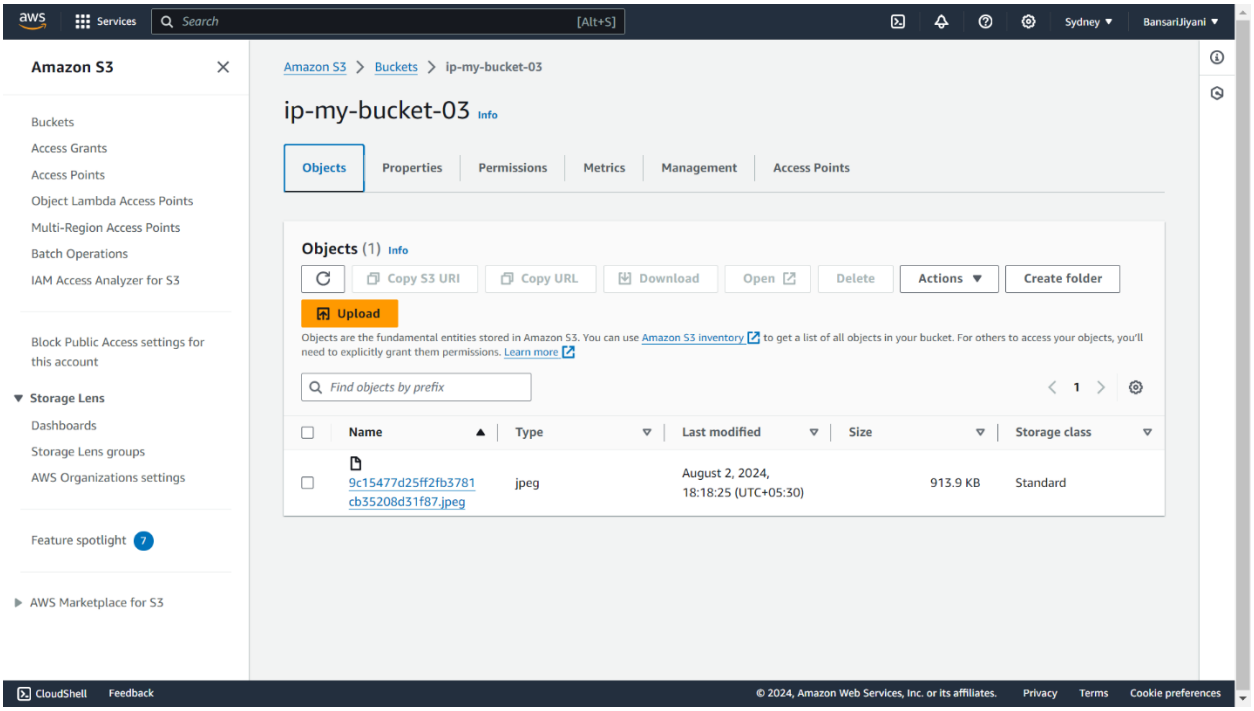

Use multiple statements to add permissions for more than one serv
1 Action(s) Selected
All A
n:aws:s3:::ip-my-bucket-03/*
ARN should follow the following format: arn:aws:s3:::${BucketNan
Use a comma to separate multiple values.
Add Conditions (Optional)
Add Statement



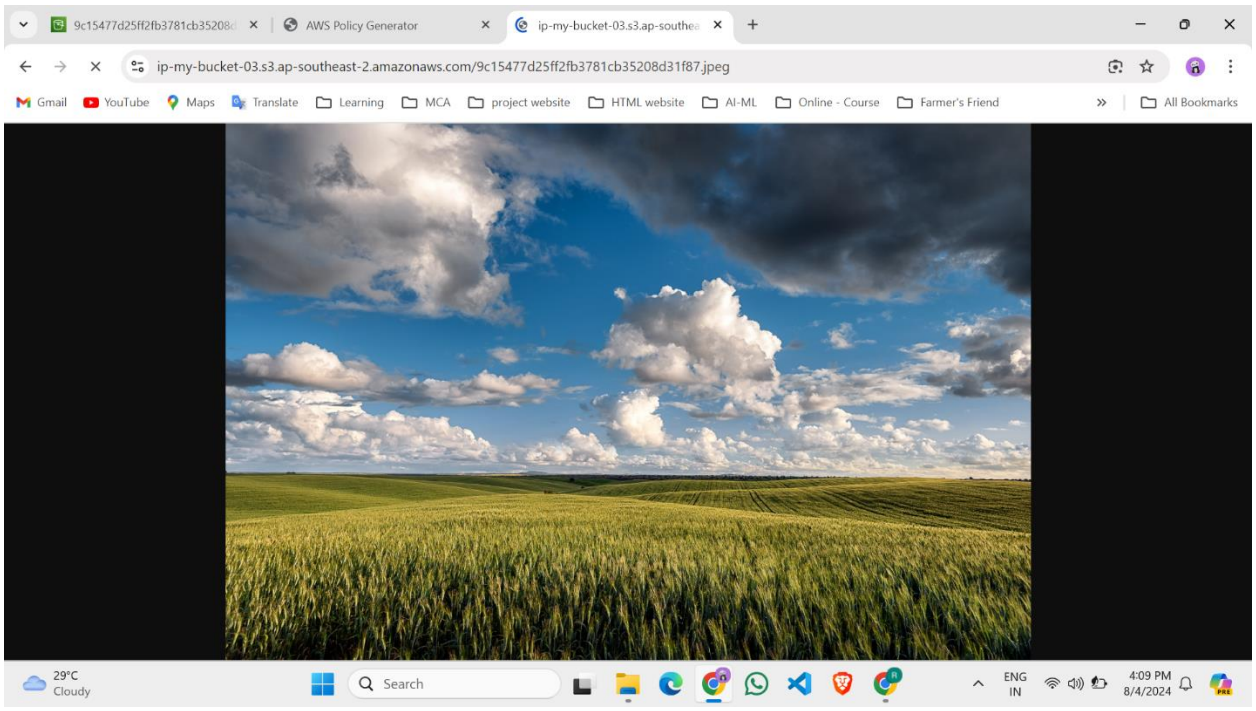
7. **Click on Add statement and Get this code . Copy it and paste it in Bucket Policy and Save Changes.**





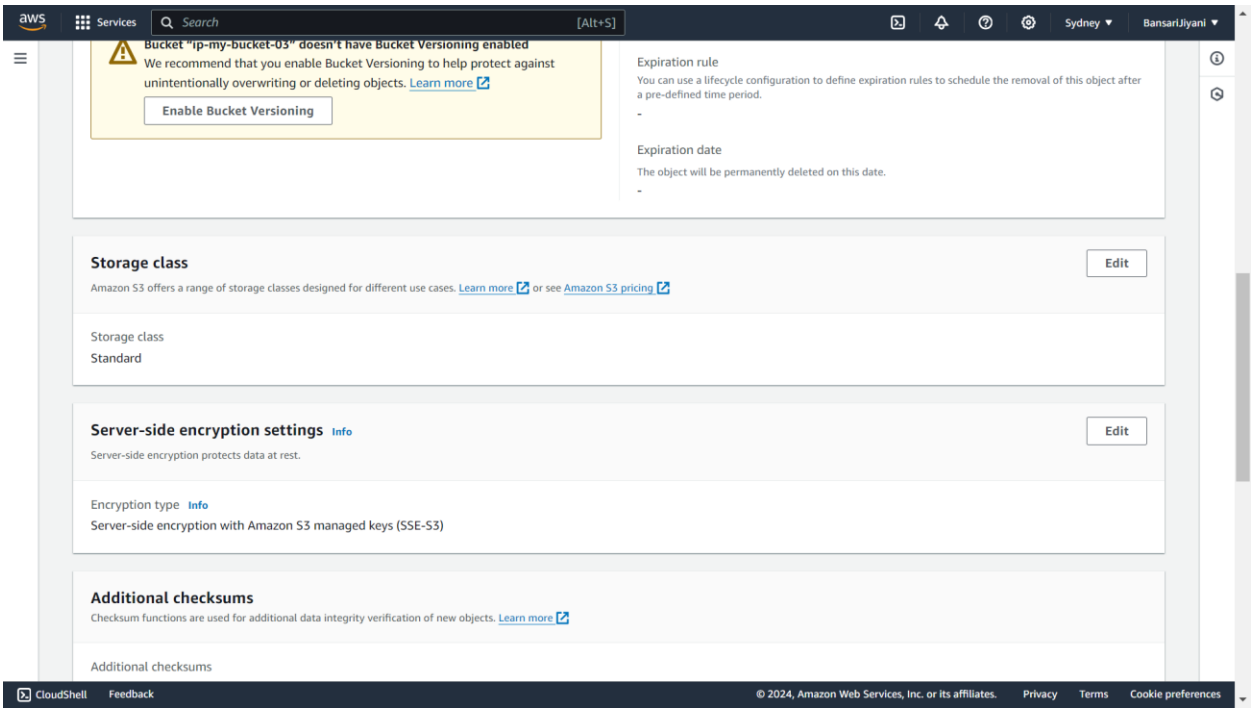


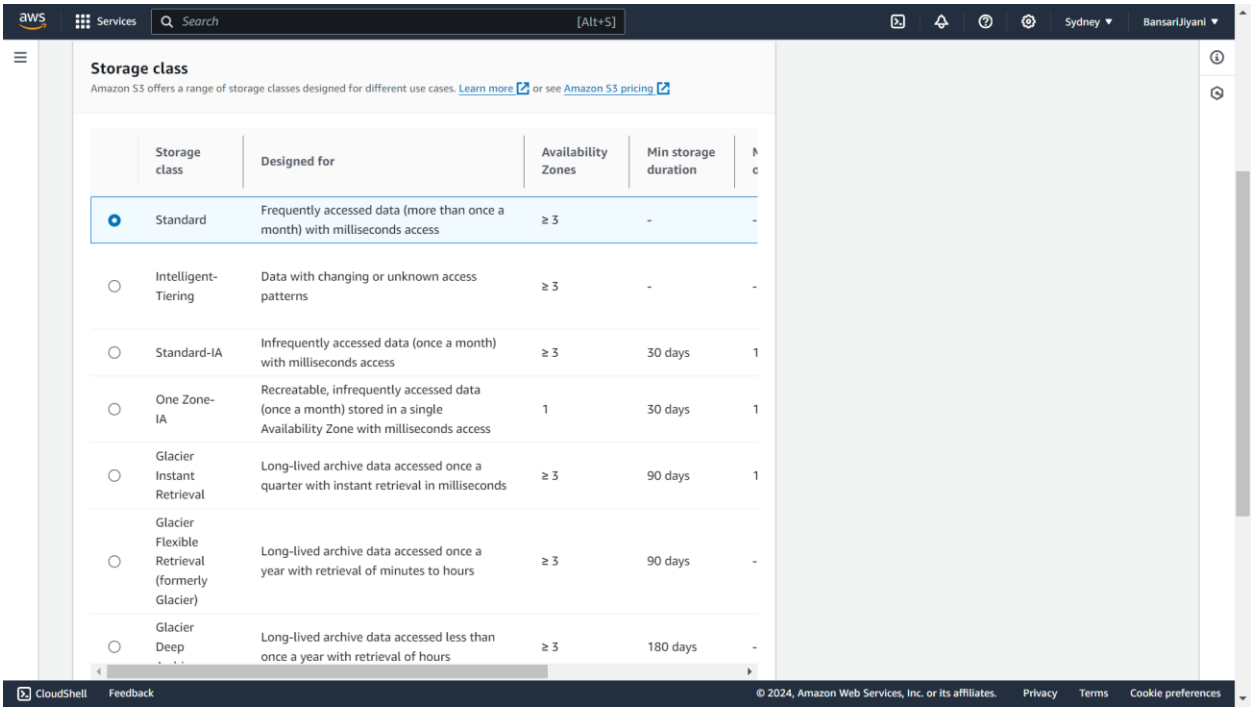
8. **Now Copy the object URL and Paste it in other Page And now You can See the object**


9c15477d25ff2fb3781cb35208
AWS Policy Generator
ip-my-bucket-03.s3.ap-southea
ip-my-bucket-03.s3.ap-southeast-2.amazonaws.com/9c15477d25ff2fb3781cb35208d31f87.jpeg
Gmail
YouTube
Maps
Translate
Learning
MCA
project website
HTML website
AI-ML
Online - Course
Farmer's Friend
All Bookmarks
29°C
Cloudy
Search
ENG
IN
4:09 PM
8/4/2024

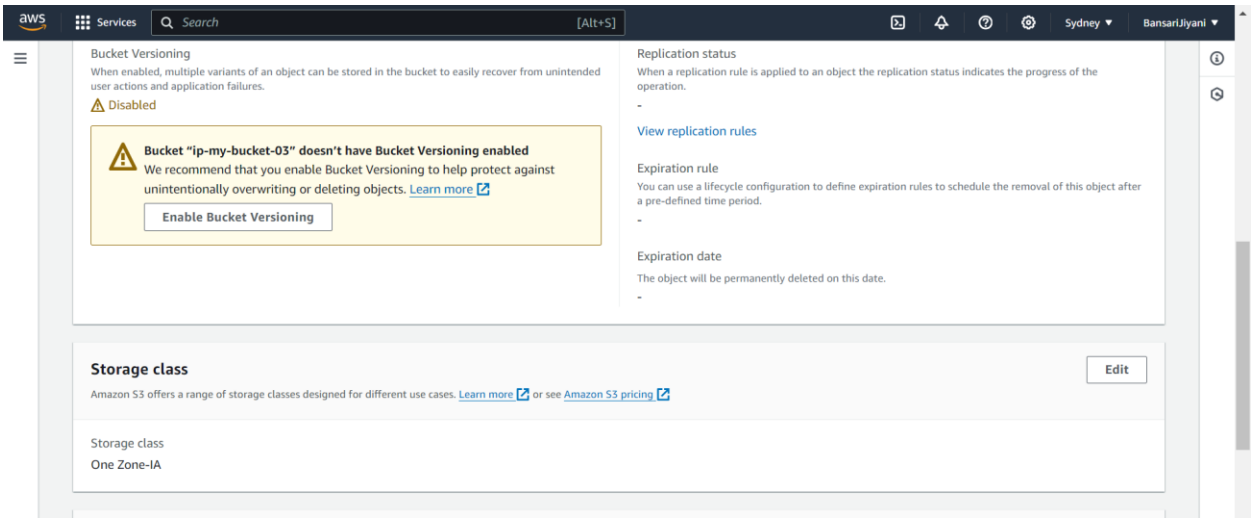
Storage Classes

1. **Create One bucket And Upload Any file and got the object Properties.and Go to the Storage class**

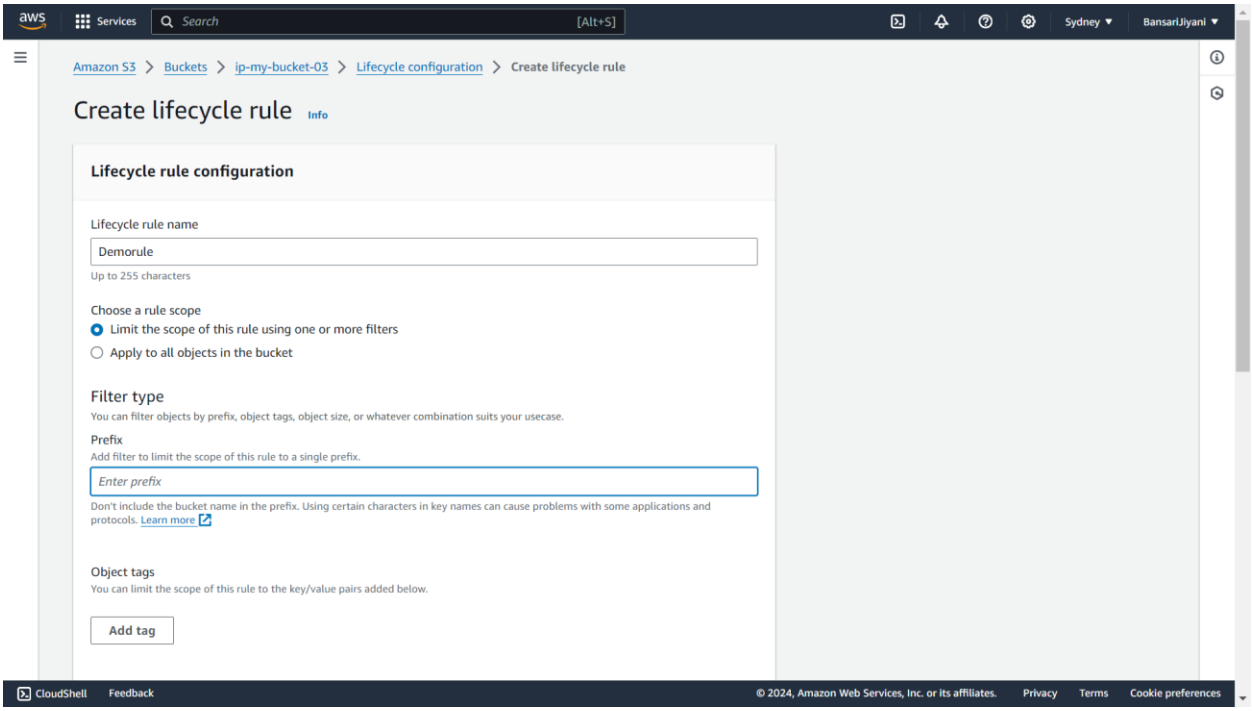




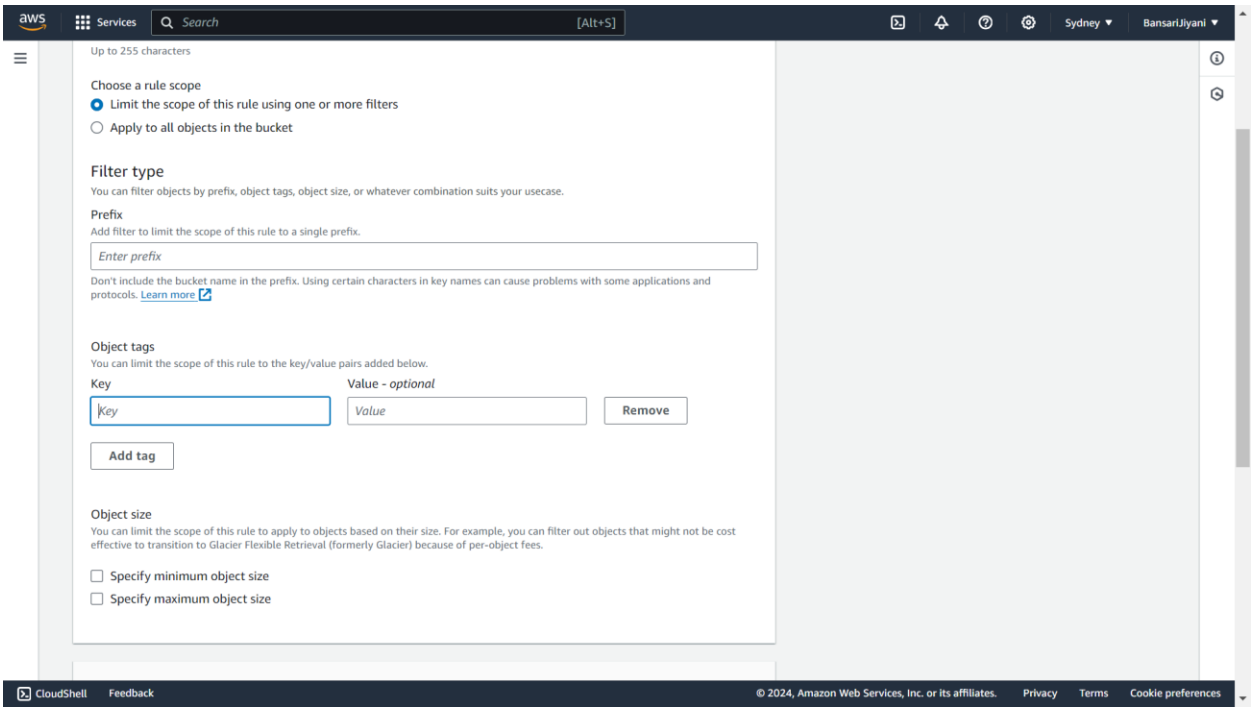
2. **Edit Standard With One-Zone-IA**



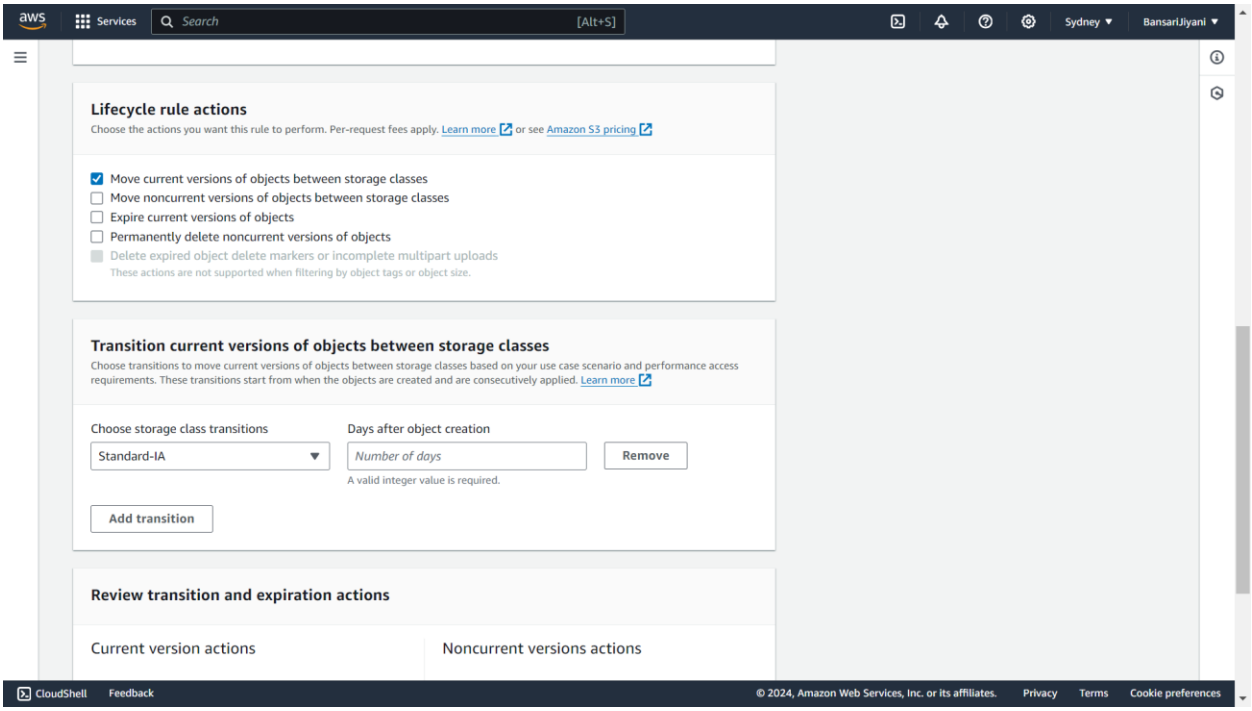
3. **Got to the Management of bucket and Create a Lifecycle as per your choice .**



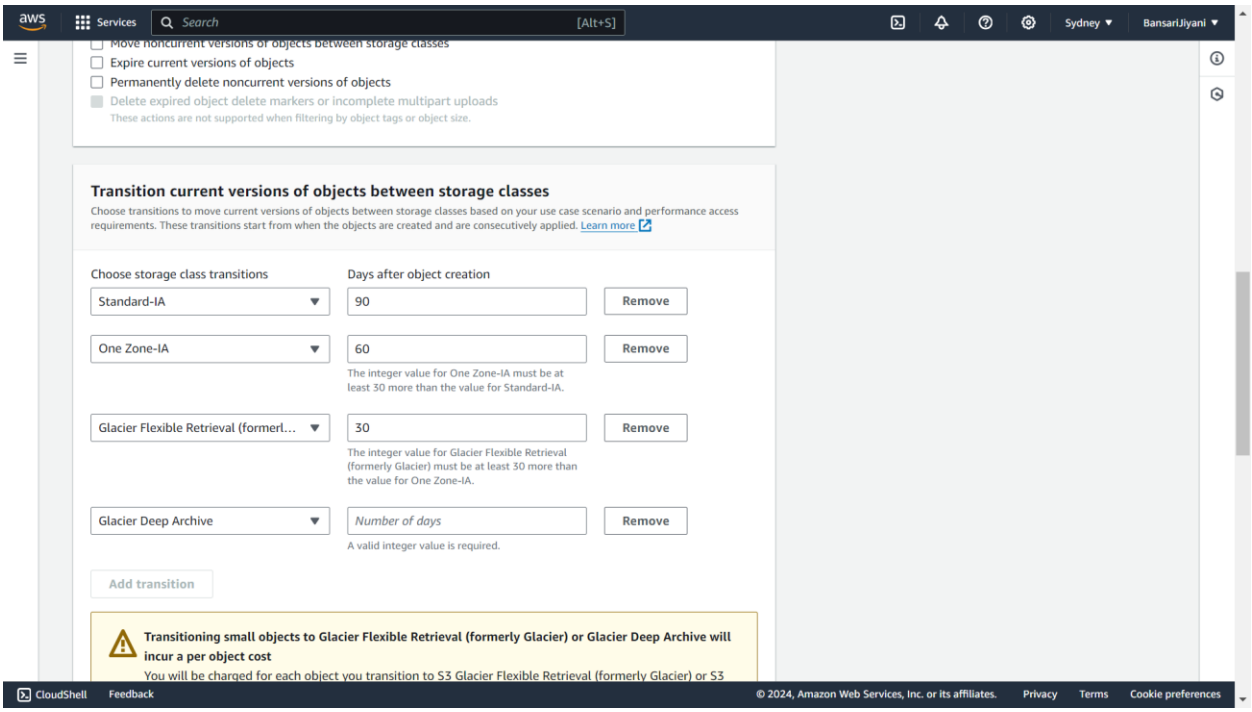
Also add the key for object



Select a Lifecycle Rule actions



Add the version of object between the Storage class like this and create a rule.

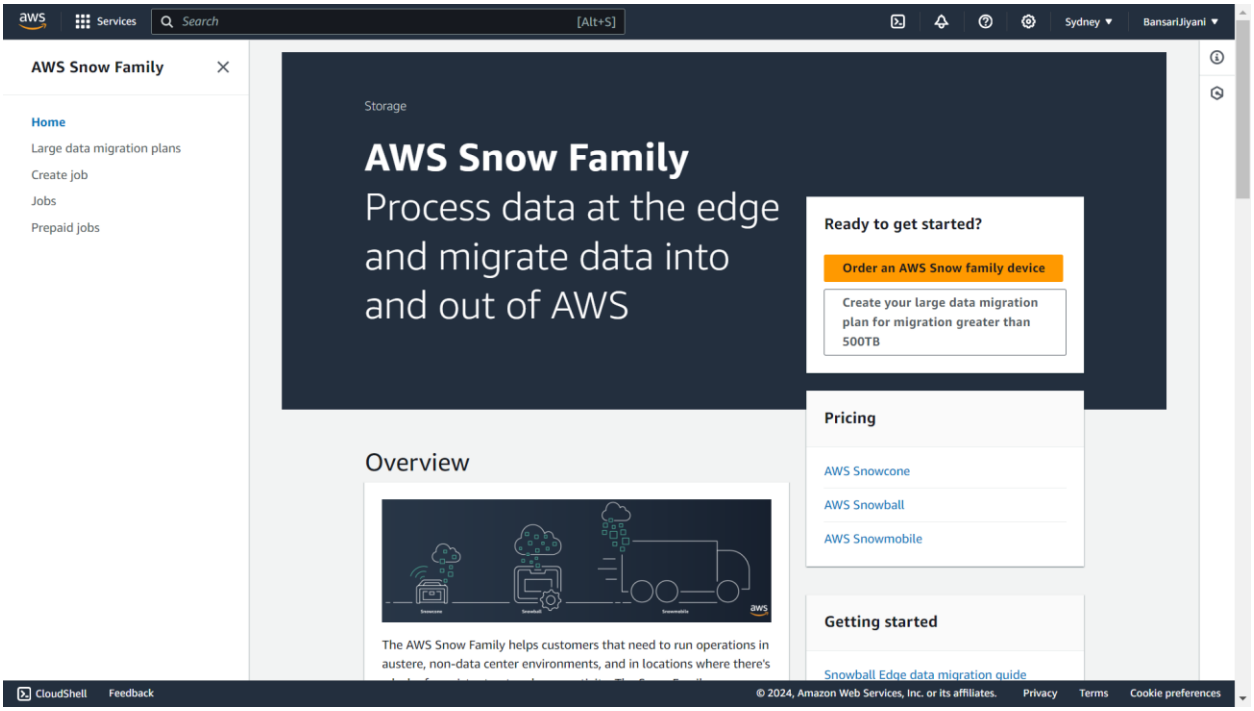


Snow Family Service

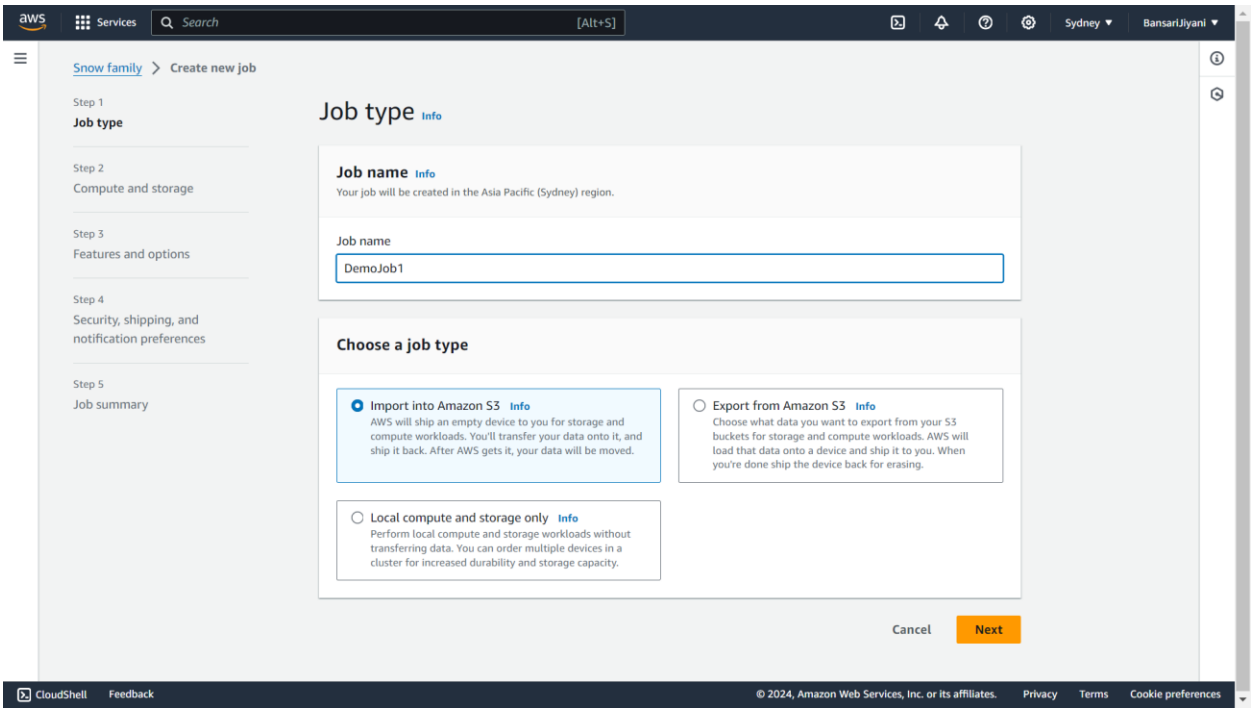
- **Description** : AWS Snow Family is a service for customers who want to transport terabytes or petabytes of data to and from AWS, or who want to access the storage and compute power of the AWS Cloud locally and cost effectively in places where connecting to the internet might not be an option.

- **PRACTICAL :**

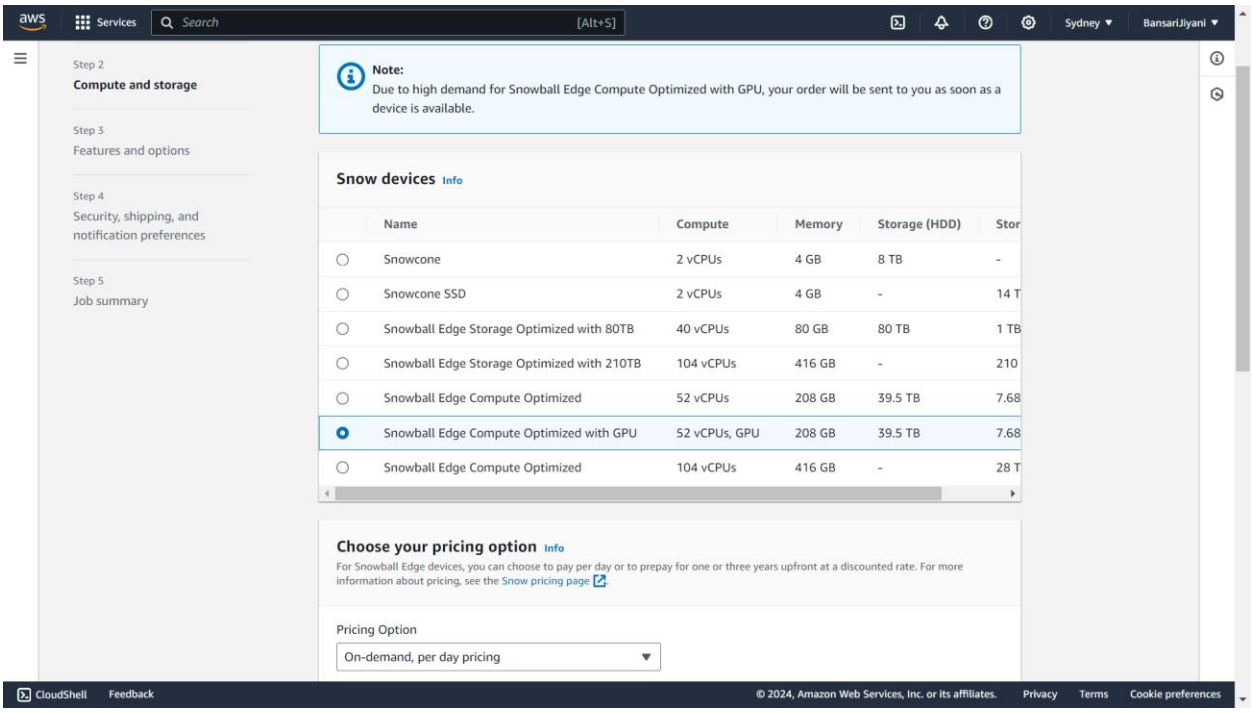
1. **Search Snow Family Device and Order an AWS snow Family Device**



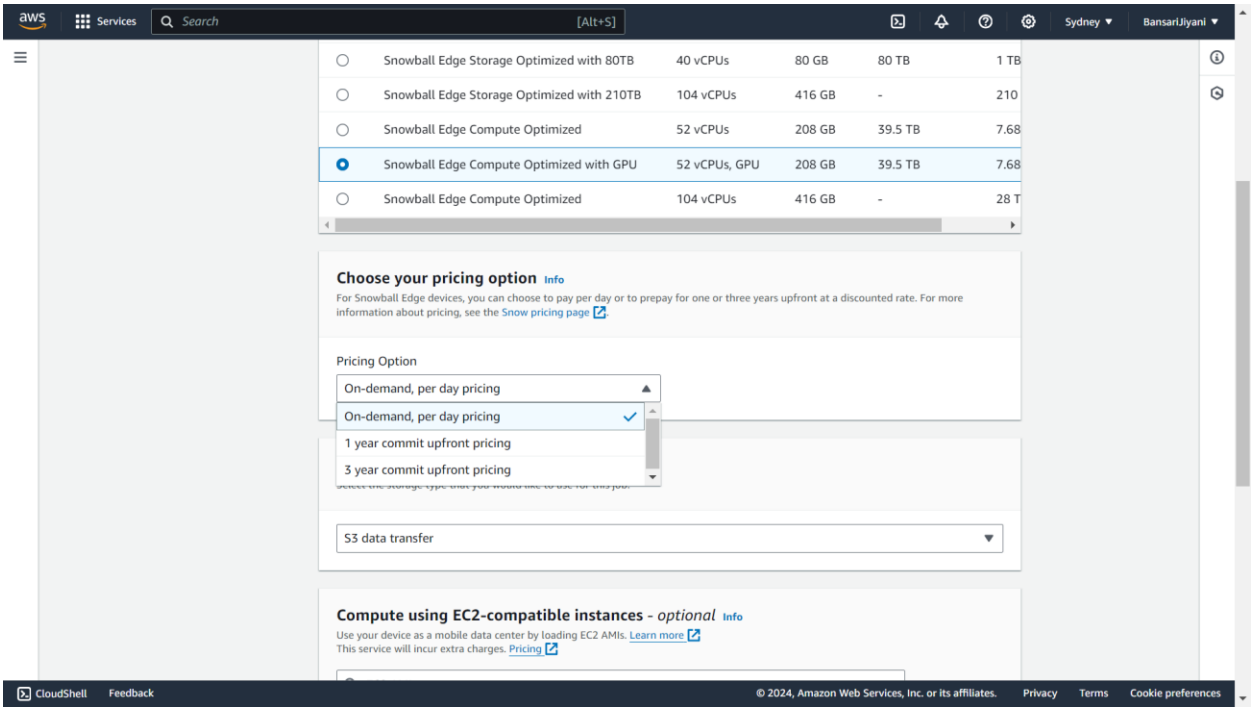
2. Give the Job name and Select option For a job type and go -> next



3. Select any snow device as per requirements

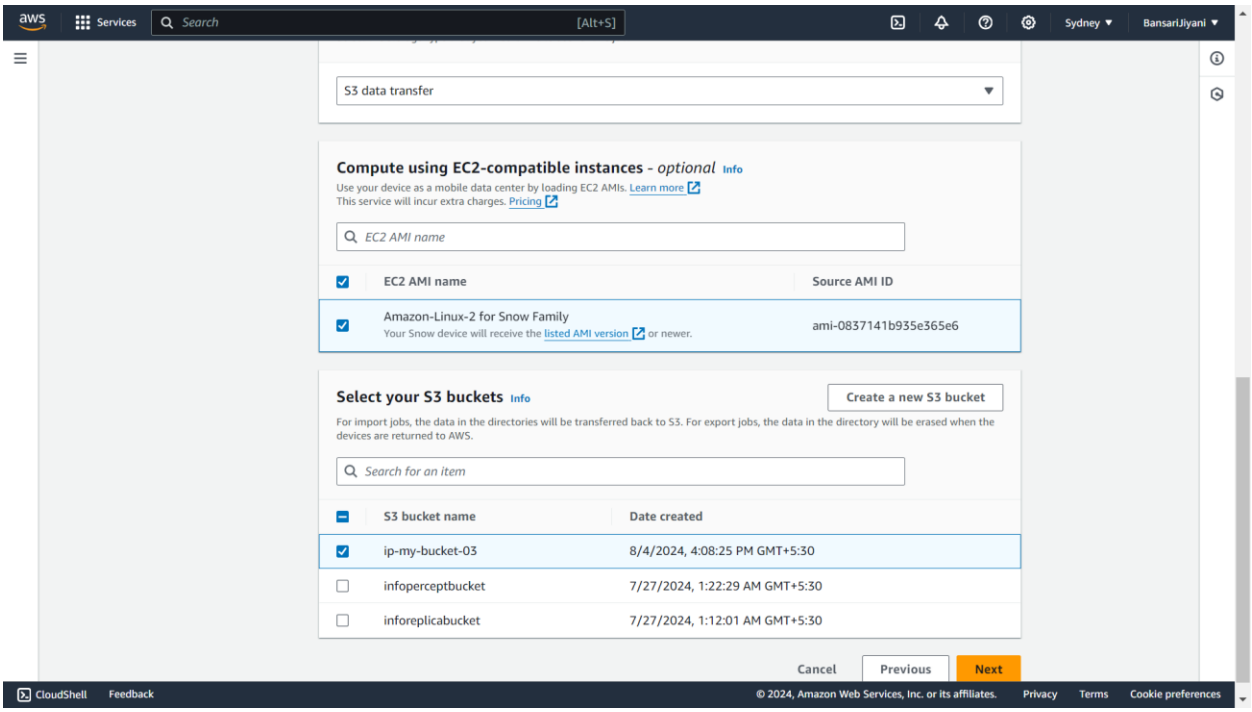


4. **Choose pricing Option and this pricing options are depends on your snow device which you choose**

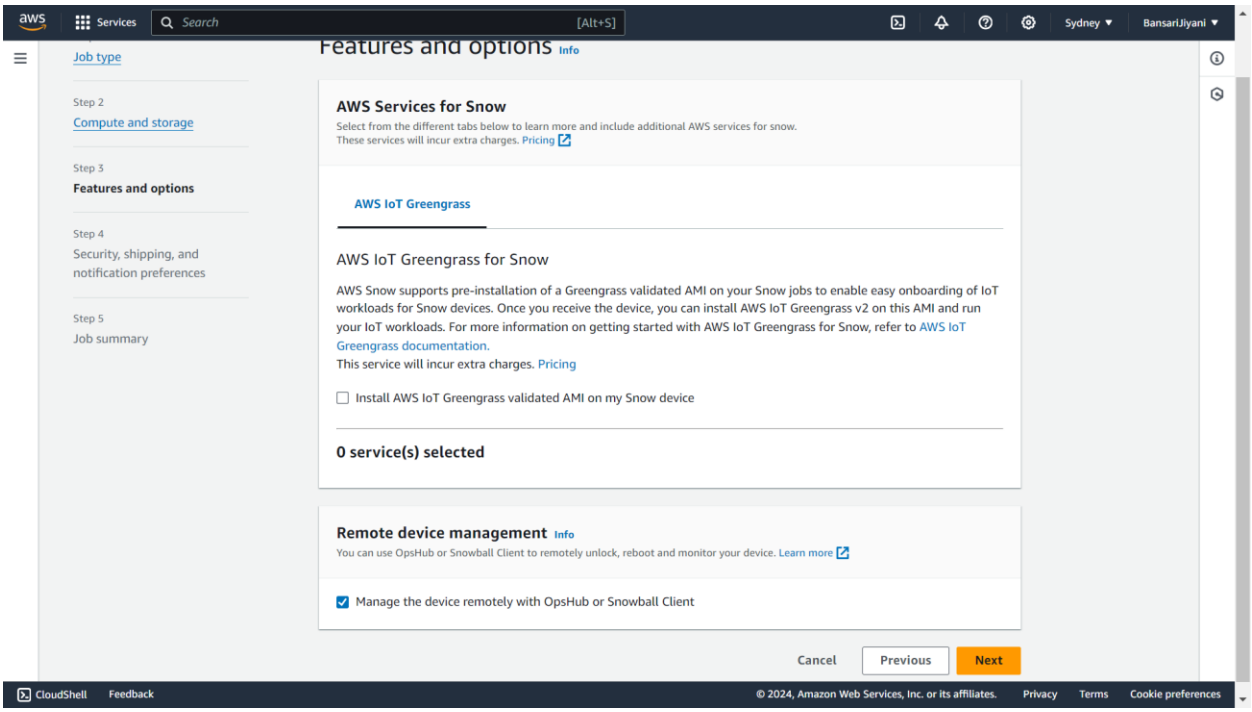


5. **Select EC2 compatible instance and that is also we change as per our personal machine.**

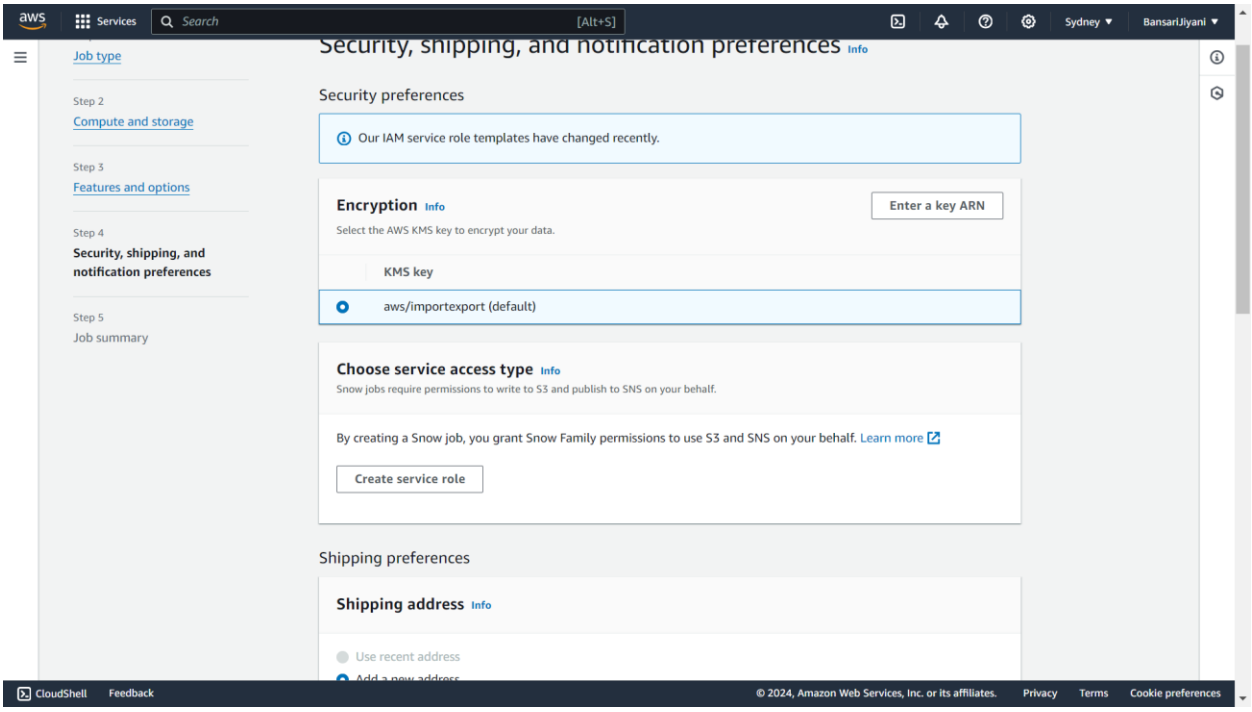
- **Select S3 bucket that where you want to put or load data**

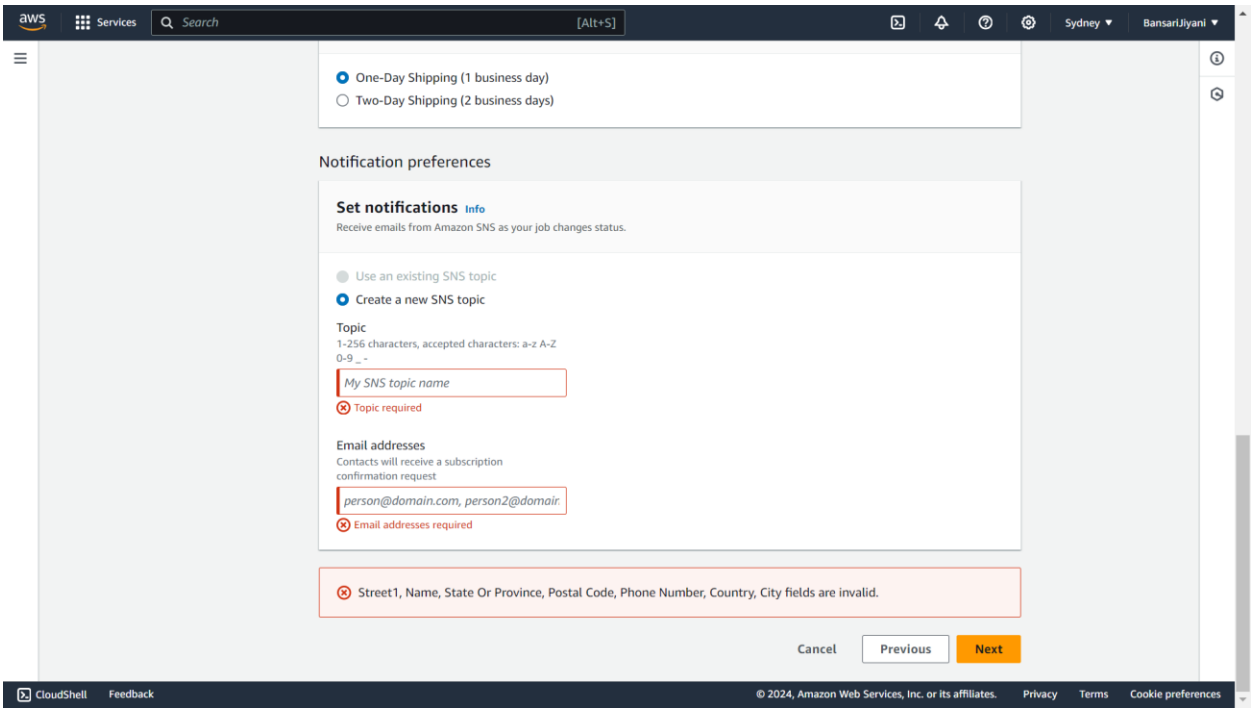


6. **Got to the next and select Remote device Management and go -> next**



7. **Select the encryption and service access type and also create a service role as per your needs and set the notification and create new SNS topic And Give SNS topic name and Email address.**





- **What is Edge computing**

➢ Edge computing in AWS is a powerful approach to building and deploying applications that require low-latency access to data and resources. By utilizing AWS services like Outposts, Local Zones, Wavelength, and IoT Greengrass, businesses can optimize their infrastructure to deliver faster, more reliable, and cost-effective solutions. This makes edge computing an essential strategy for modern applications that demand high performance and real-time processing.