

**Cloud Computing Architecture Lab**

**Name:** Pratham Kandari

**Sap Id:** 500097663

**Batch:** 7

**Experiment -9**

**i)Replicate the bucket in the same region and different region. ii) Delete the object through Lifecycle rule creation. iii) Create a transition action to move the object from one storage class to another.**

**Q1)** **Why we have different storage classes in S3 and explain these in detail.**

**ANS)** Amazon S3 offers several different storage classes designed to help customers optimize their costs and performance based on the specific needs of their data. Each storage class has its own characteristics and access patterns, and choosing the right one can significantly impact the cost and performance of your S3 usage.

The following are the different storage classes available in S3, along with a brief description of each:

1. S3 Standard: This is the default storage class for S3. It provides high durability, availability, and performance for frequently accessed data. S3 Standard is suitable for a wide range of use cases, including big data analytics, mobile and gaming applications, content distribution, and backup and recovery.
2. S3 Intelligent-Tiering: This storage class is designed to automatically move objects between two access tiers based on changing access patterns. It uses machine learning algorithms to analyze usage patterns and optimize costs while maintaining high performance and availability. S3 Intelligent-Tiering is ideal for workloads with unknown or unpredictable access patterns.
3. S3 Standard-Infrequent Access (S3 Standard-IA): This storage class provides the same high durability, availability, and performance as S3 Standard, but at a lower cost for infrequently accessed data. S3 Standard-IA is suitable for long-term storage, backups, and disaster recovery data.
4. S3 One Zone-Infrequent Access (S3 One Zone-IA): This is a lower-cost version of S3 Standard-IA that stores data in a single availability zone, rather than across multiple zones. It offers the same durability and performance as S3 Standard-IA but with a lower availability guarantee. S3 One Zone-IA is suitable for data that can be recreated if lost.
5. S3 Glacier: This storage class provides extremely low-cost storage for data archiving and long-term backup. It offers low retrieval times (within minutes) for archived data and can be used for regulatory compliance and other use cases that require long-term data retention.
6. S3 Glacier Deep Archive: This is the lowest-cost storage class in S3, designed for long-term data retention and archiving. Retrieval times can take several hours, but the cost per GB is significantly lower than any other S3 storage class. S3 Glacier Deep Archive is suitable for compliance, historical, and other low-cost, infrequently accessed data.

In summary, choosing the right storage class in S3 depends on your specific needs, access patterns, and budget. By understanding the characteristics of each storage class, you can optimize your costs and performance to meet your business requirements.

**Q2) What do you understand by lifecycle management in S3.**

**ANS)** Lifecycle management in Amazon S3 is a feature that allows you to automate the process of moving objects between different storage classes or deleting them based on predefined rules. This feature can help you optimize your storage costs and simplify data management by automating the transition of objects to different storage classes or deleting them at the end of their lifecycle.

With S3 lifecycle management, you can define lifecycle policies that apply to a specific bucket or a subset of objects within a bucket. You can define lifecycle policies to transition objects to different storage classes based on their age or based on other criteria such as their size, whether they are encrypted or not, or whether they have been accessed recently.

For example, you might define a lifecycle policy that automatically moves objects to the S3 Standard-Infrequent Access (S3 Standard-IA) storage class after 30 days and to the S3 Glacier storage class after 90 days. This policy would help you reduce storage costs by automatically transitioning less frequently accessed objects to lower-cost storage classes.

You can also define lifecycle policies that automatically delete objects after a certain period of time or after they have reached a specific age or size. This can help you ensure that objects are deleted at the end of their lifecycle, reducing storage costs and improving data security.

In summary, S3 lifecycle management is a powerful feature that enables you to automate the process of moving objects between different storage classes or deleting them based on predefined rules. By defining lifecycle policies, you can optimize your storage costs, simplify data management, and ensure that objects are deleted at the end of their lifecycle.

**Q3) What do you understand by replication rules in S3.**

**ANS)** Replication rules in Amazon S3 is a feature that allows you to automatically replicate your data from one S3 bucket to another S3 bucket in a different AWS region or within the same region. This feature can help you to increase the durability of your data and provide data protection and disaster recovery in case of data loss or service disruption.

With S3 replication rules, you can define replication policies that specify the source and destination buckets, the objects to replicate, and the frequency and priority of replication. You can also specify the storage class of the replicated objects, the encryption options, and the metadata to be included with the replicated objects.

For example, you can define a replication rule to replicate all objects in a production bucket to a backup bucket in a different region. You can specify that objects should be replicated every 15 minutes, and you can choose to replicate only objects that have changed since the last replication. You can also specify that the replicated objects should be stored in a lower-cost storage class, such as S3 Standard-Infrequent Access (S3 Standard-IA).

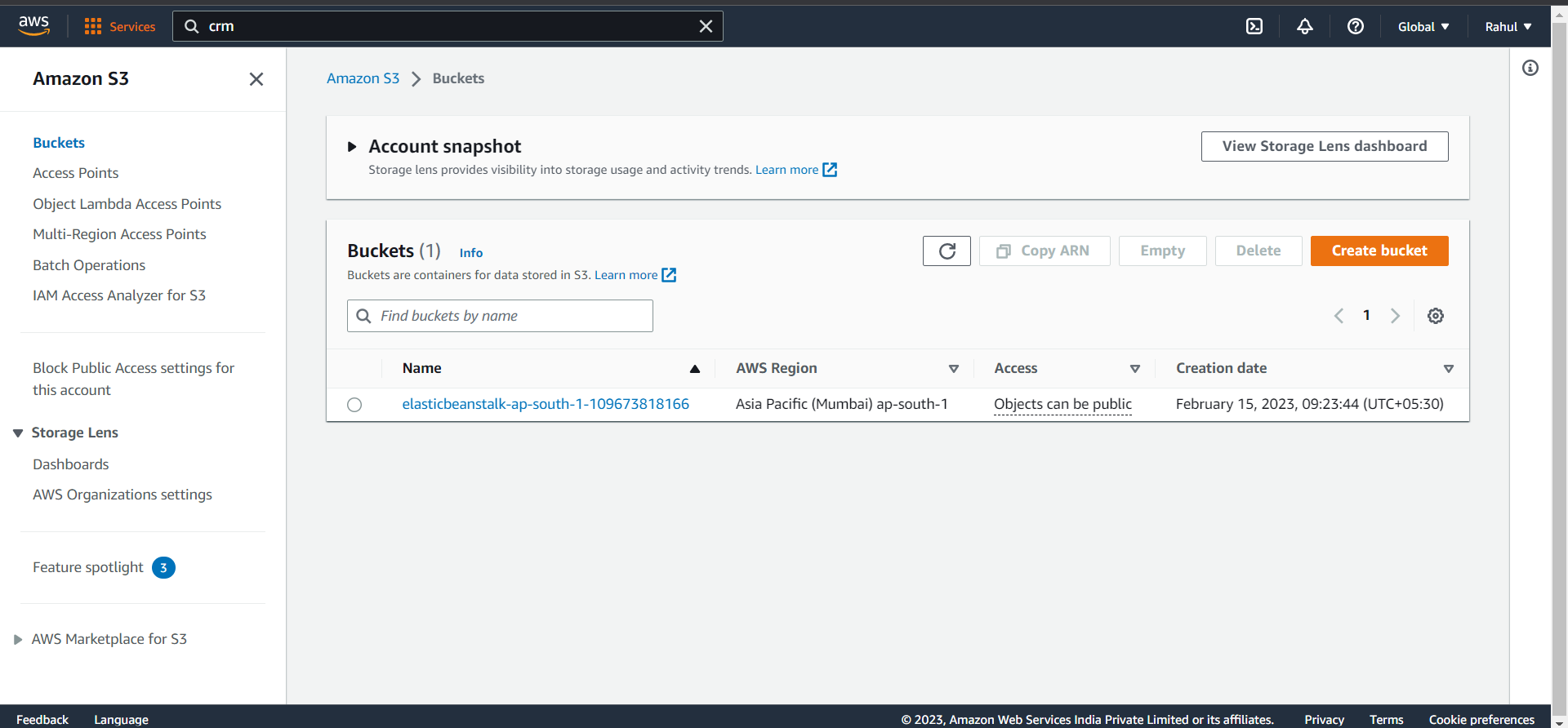
S3 replication rules provide several benefits, including:

1. Increased durability and data protection: Replicating your data to another S3 bucket can help ensure that your data is protected against data loss or service disruption.
2. Disaster recovery: Replicating your data to another AWS region can help provide disaster recovery in case of regional outages.
3. Compliance: S3 replication rules can help you comply with regulatory requirements by replicating your data to another location.

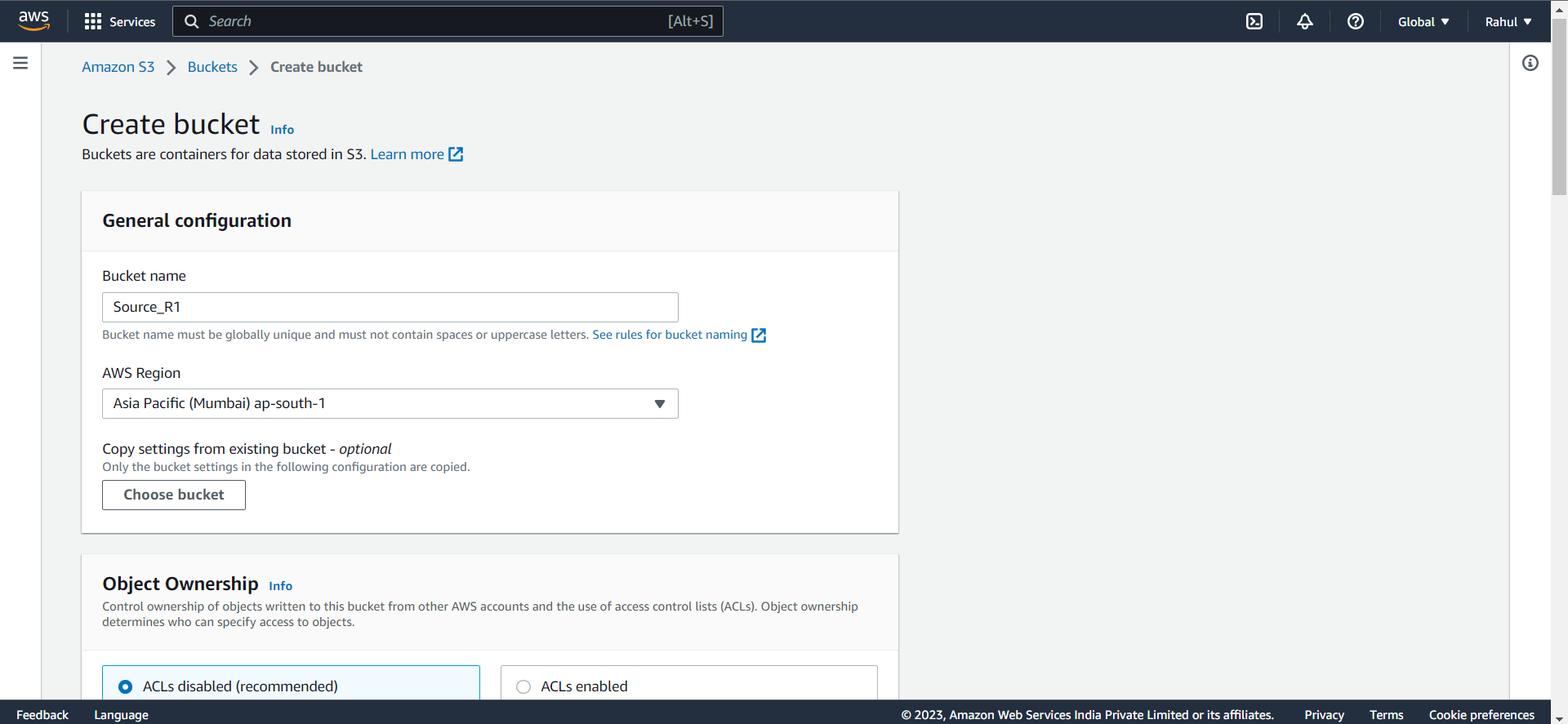
In summary, S3 replication rules is a powerful feature that allows you to automatically replicate your data from one S3 bucket to another. By defining replication policies, you can increase the durability of your data, provide data protection and disaster recovery, and comply with regulatory requirements.

**i)Replicate the bucket in the same region and different region.**

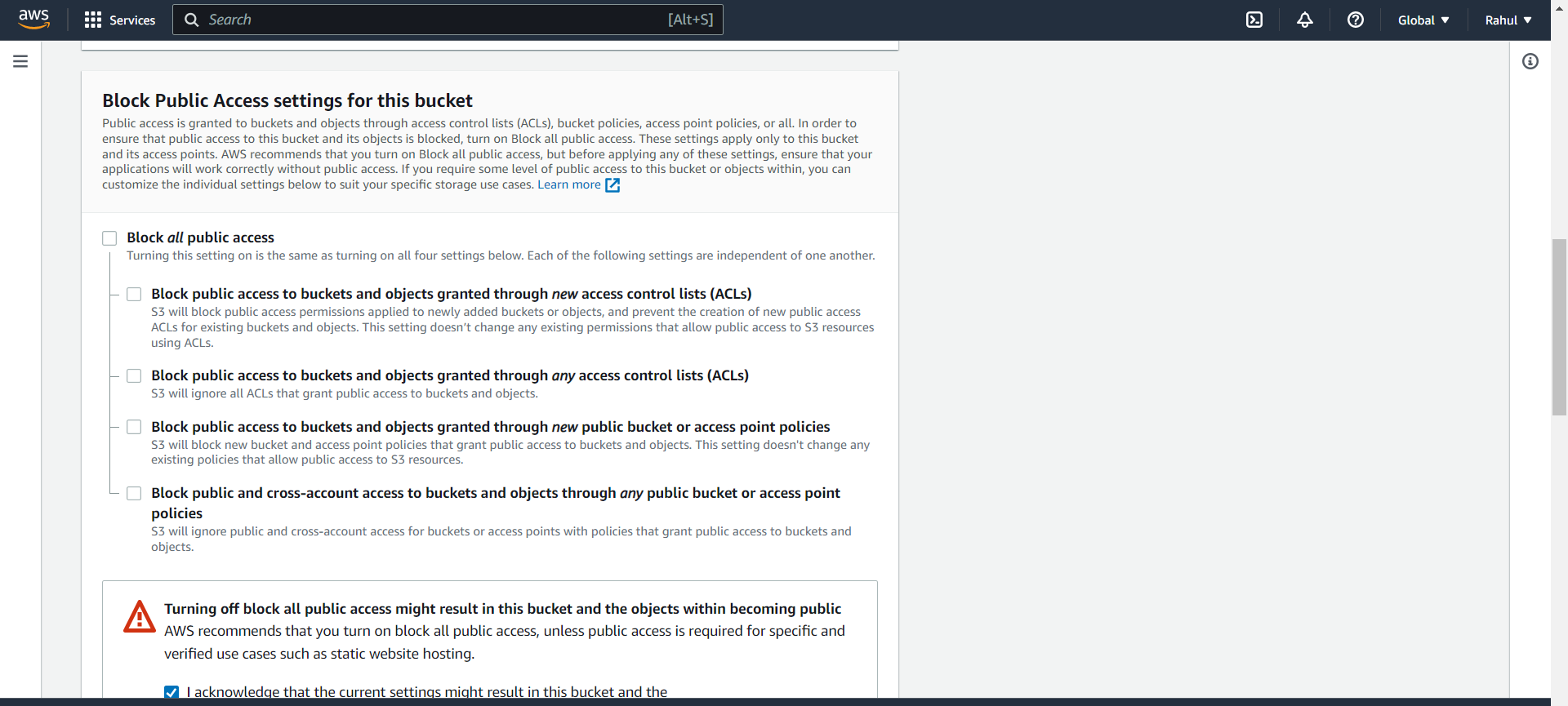
Step 1) Go to S3 and click on create bucket.



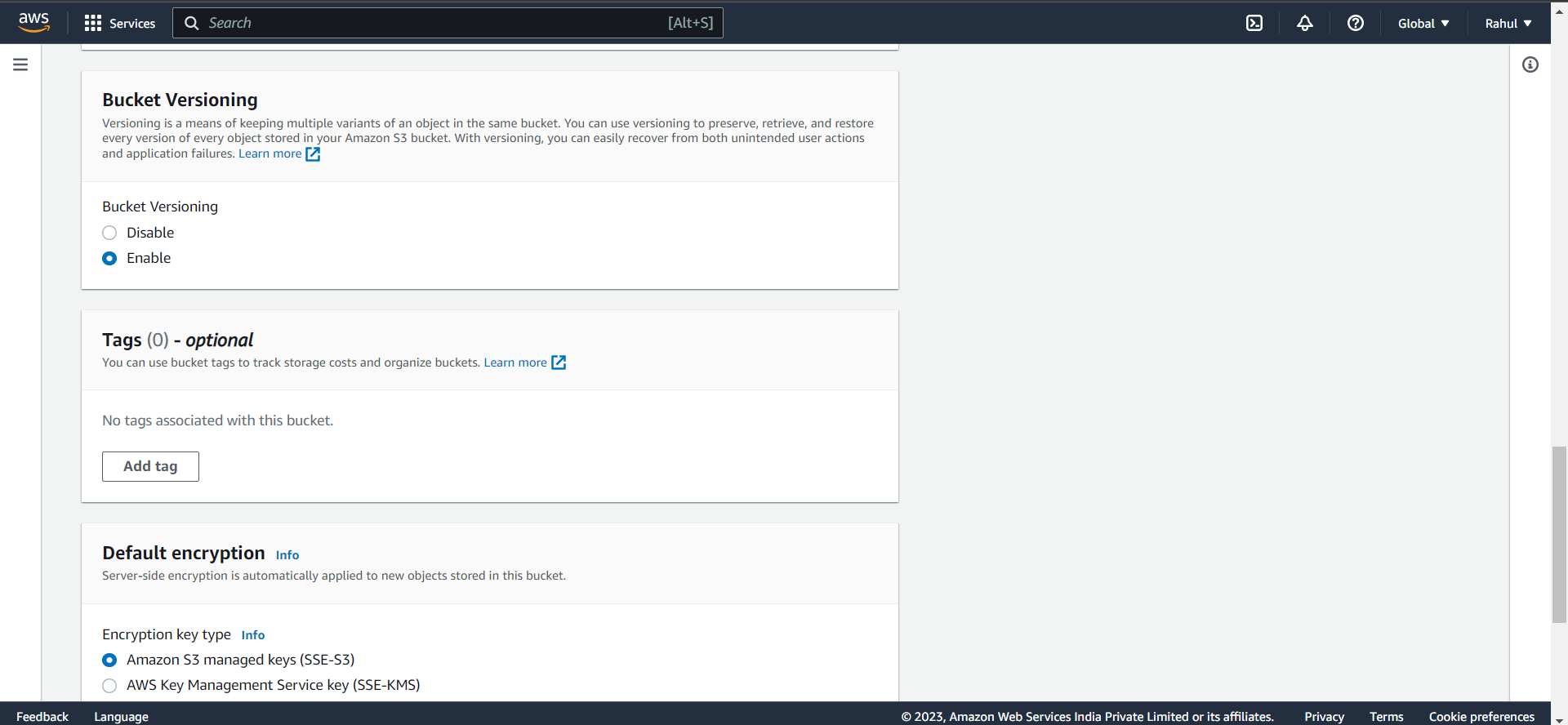
Step 2) Give it a name (Sourcebucket).



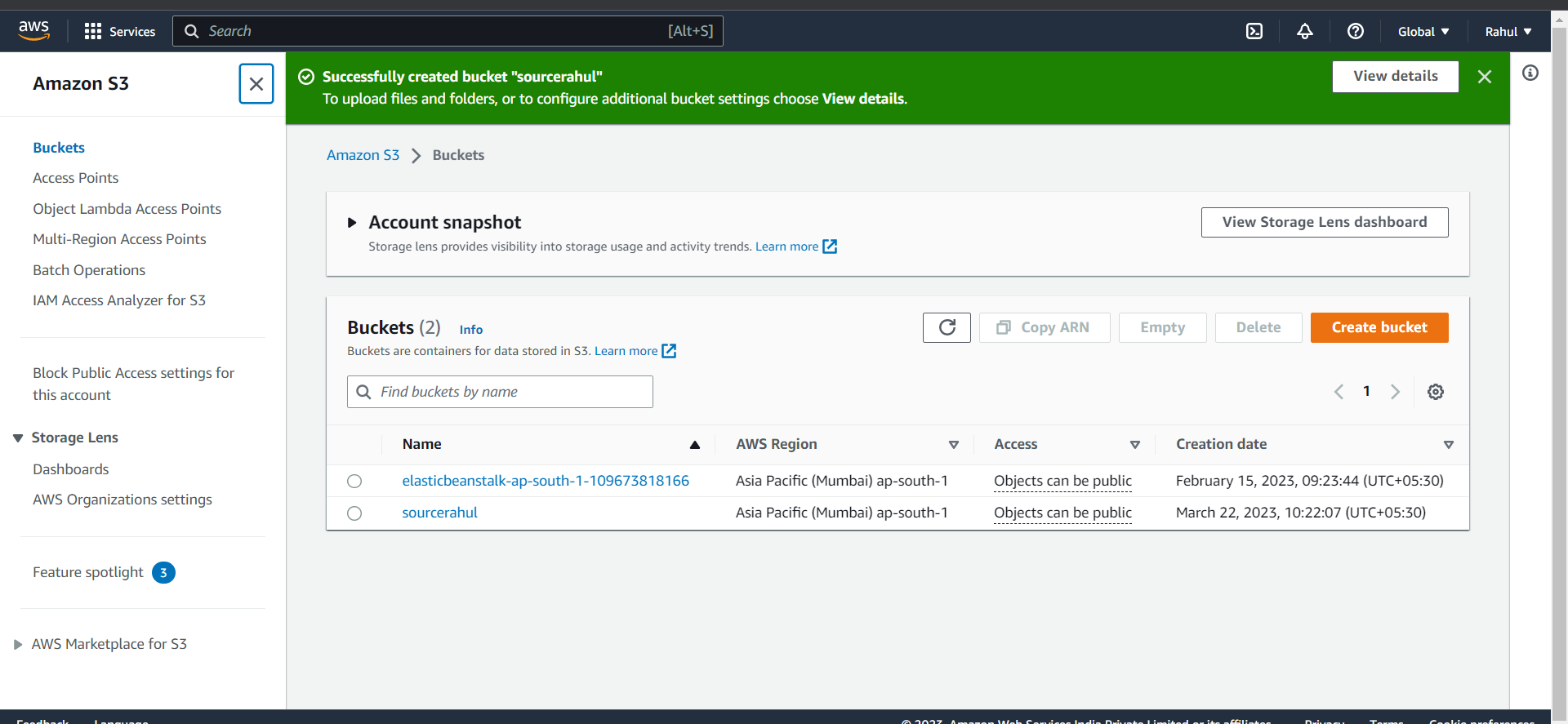
Step 3) Unblock public access.



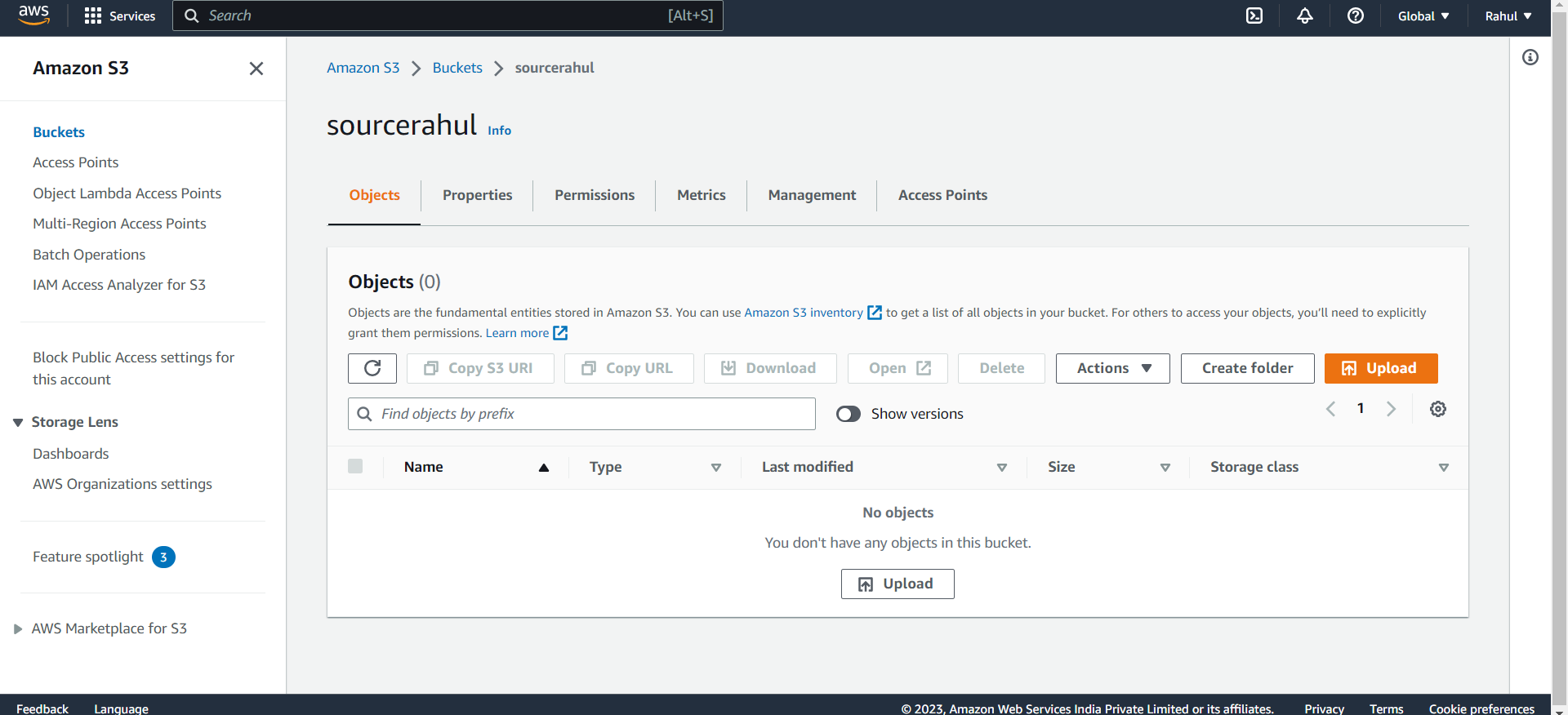
Step 4) Enable bucket versioning.



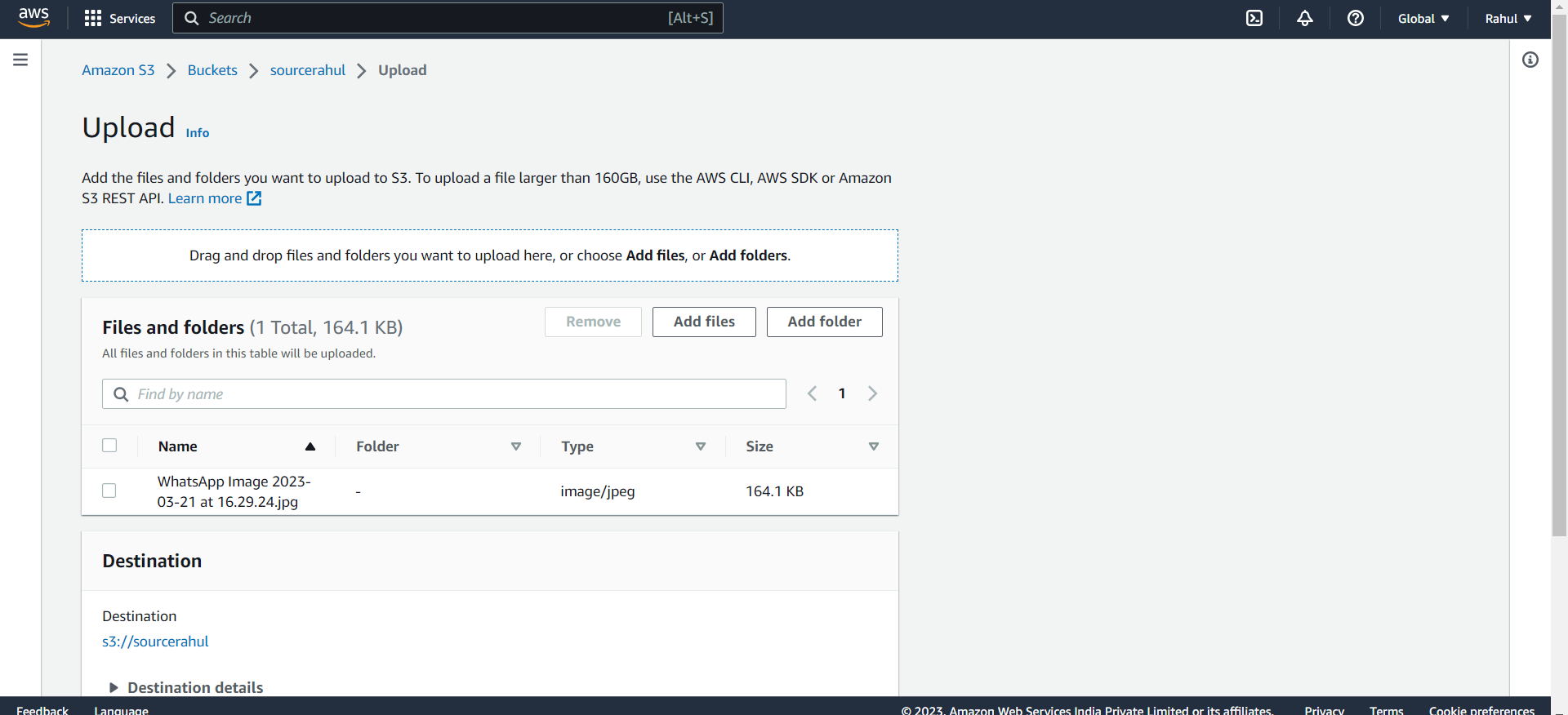
Step 5) Click on the bucket created.



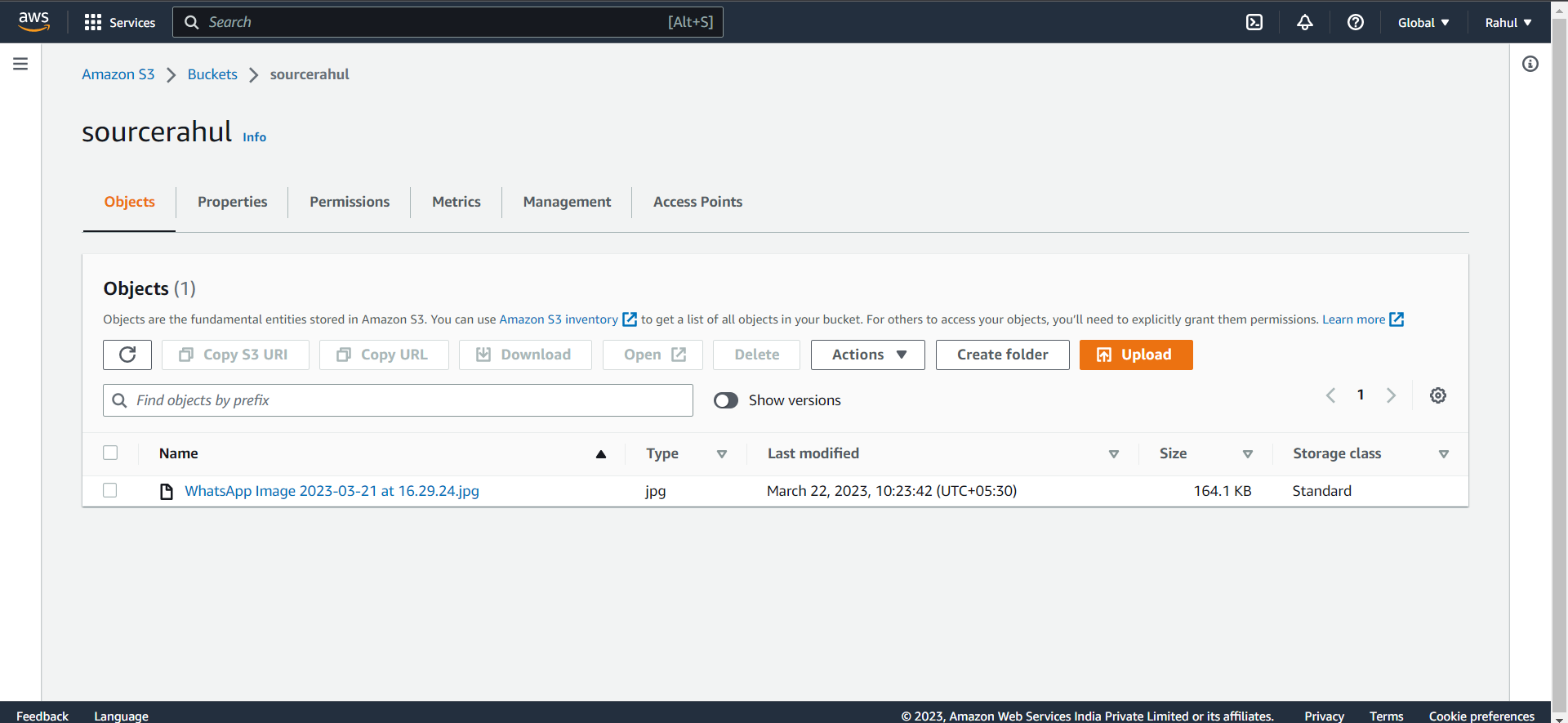
Step 6) Click on upload.



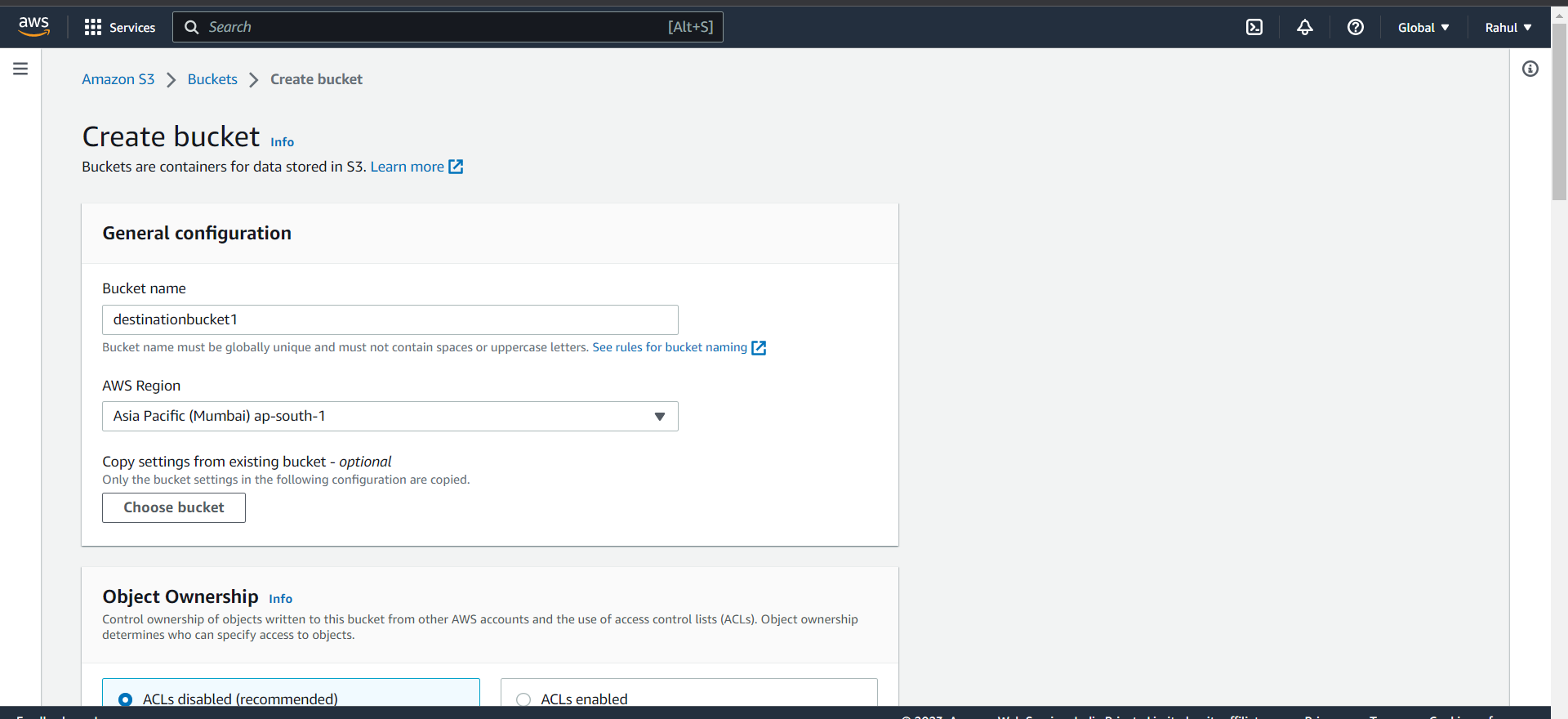
Step 7) Upload any image.



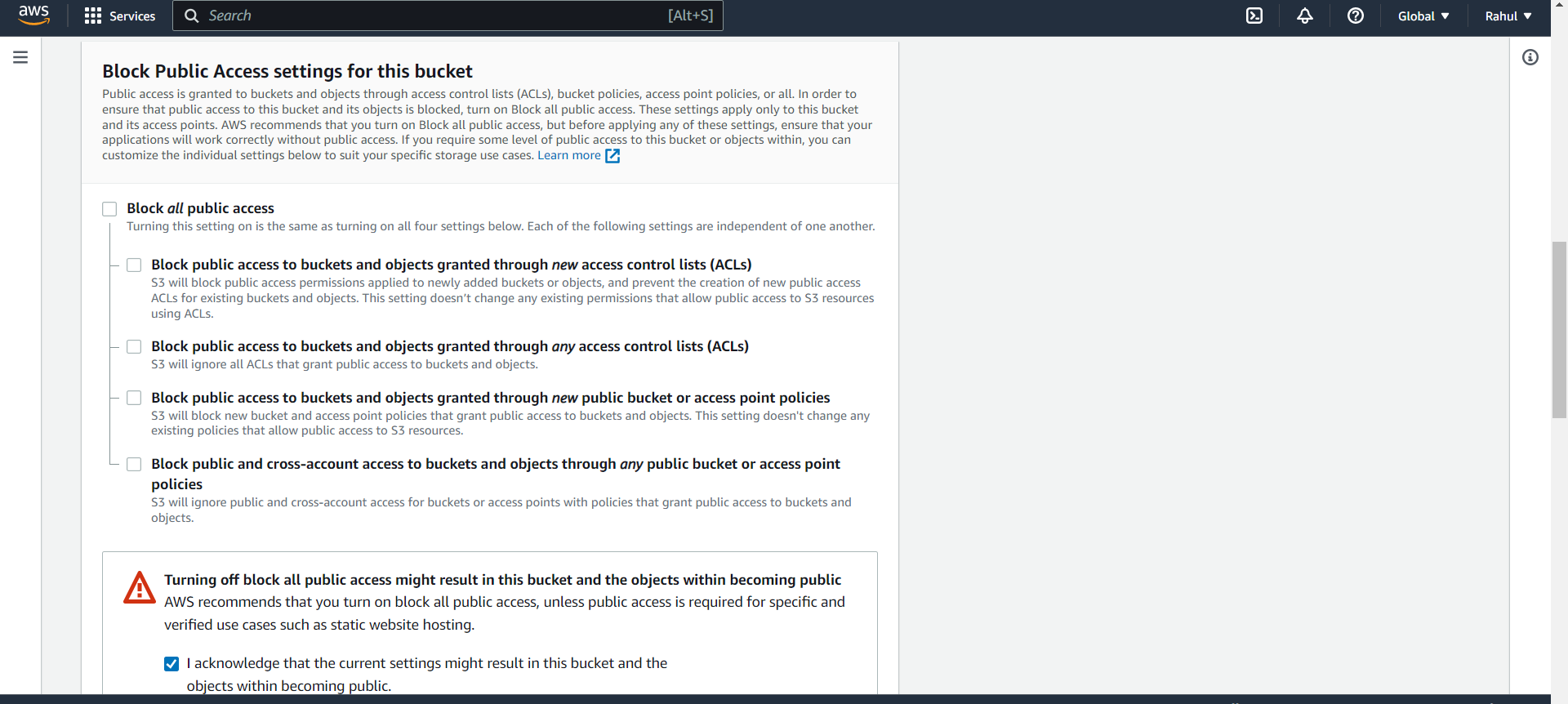
Step 8) Image will be uploaded.



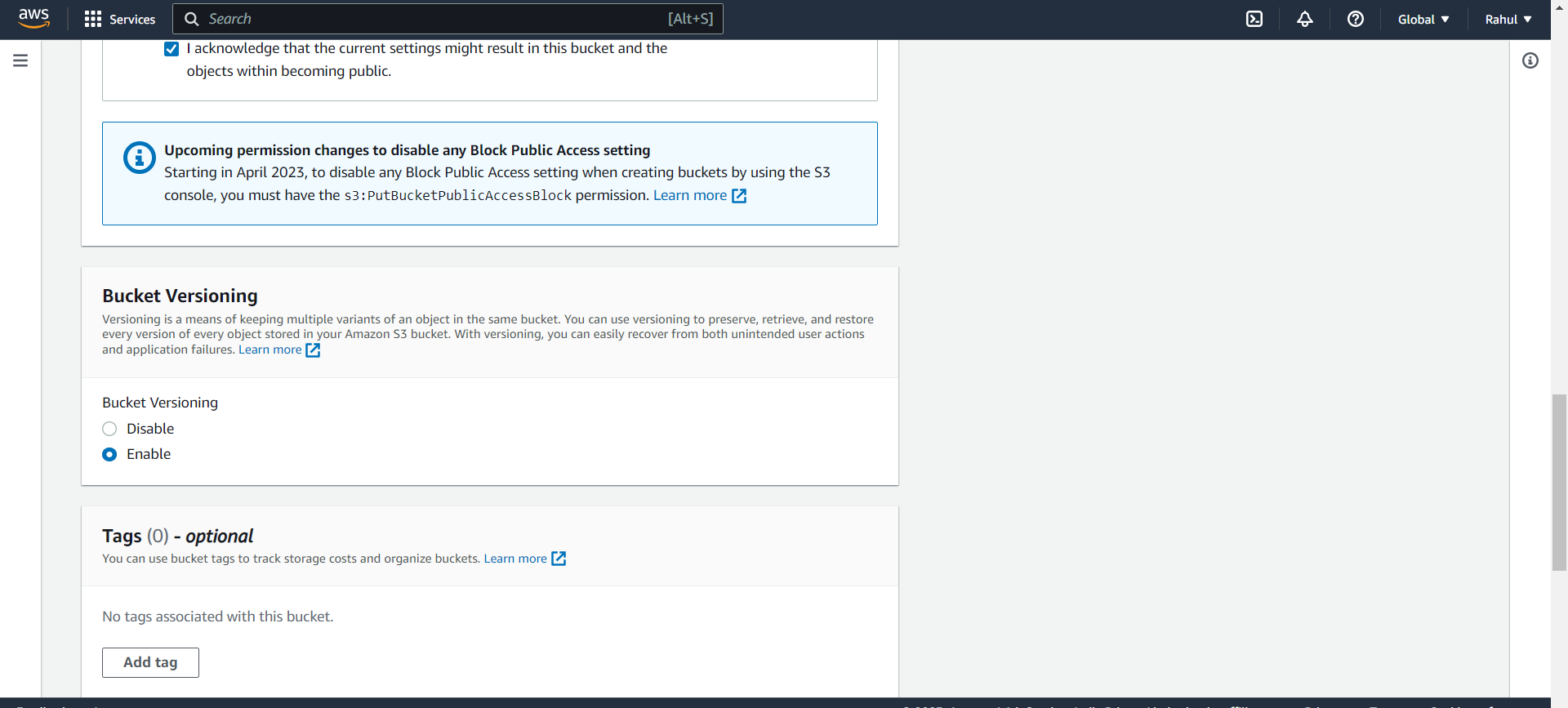
Step 9) Create another destination bucket, and give it a name(destinationbucket).



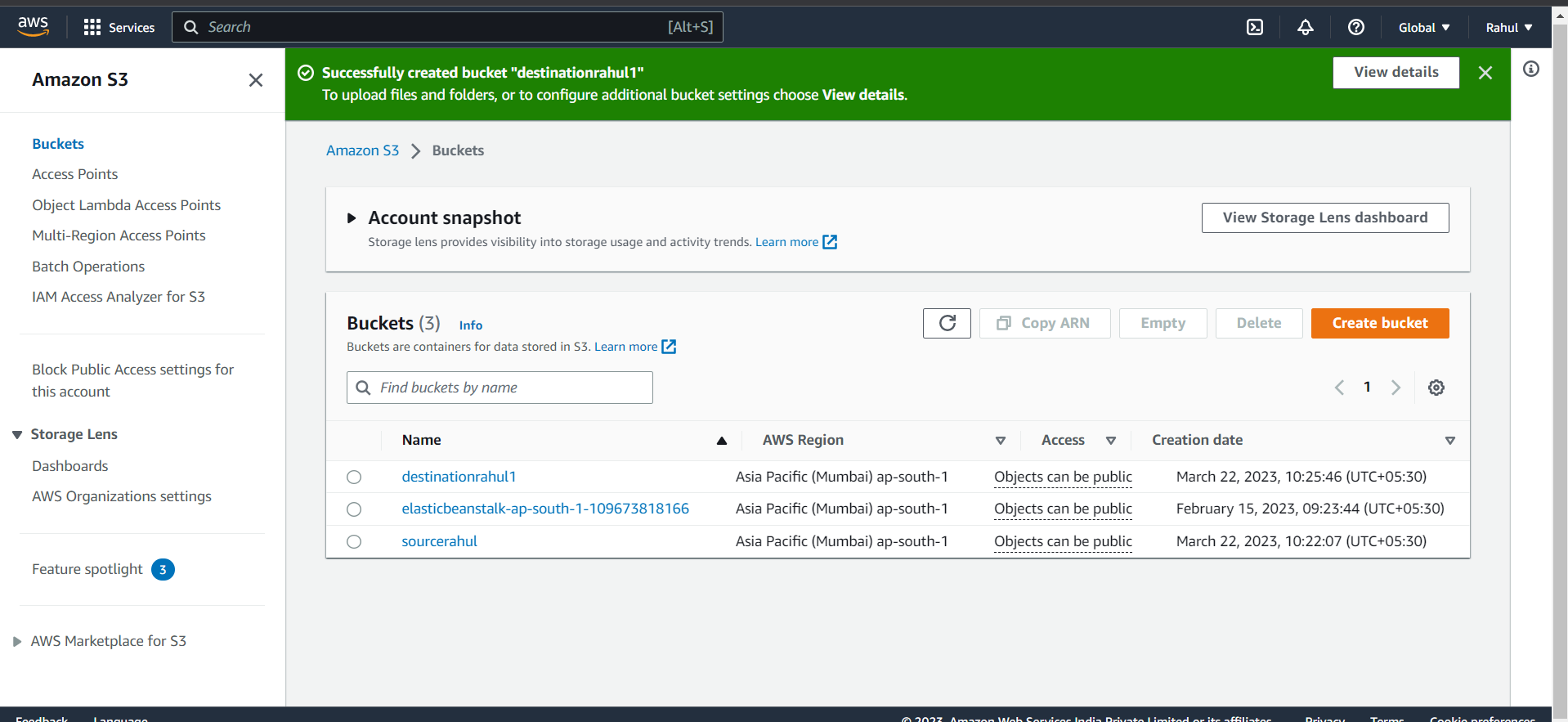
Step 10) Unblock public access.



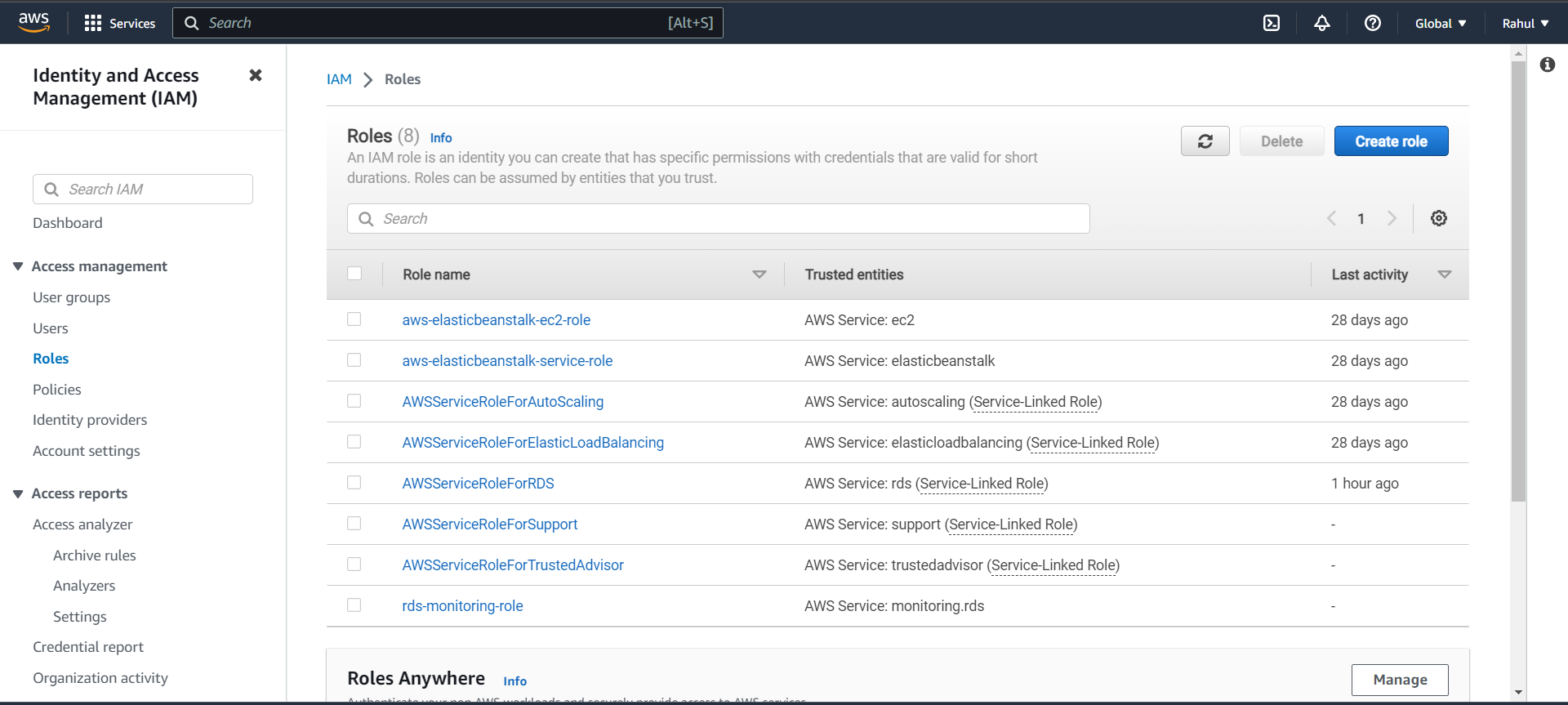
Step 11) Enable bucket versioning.



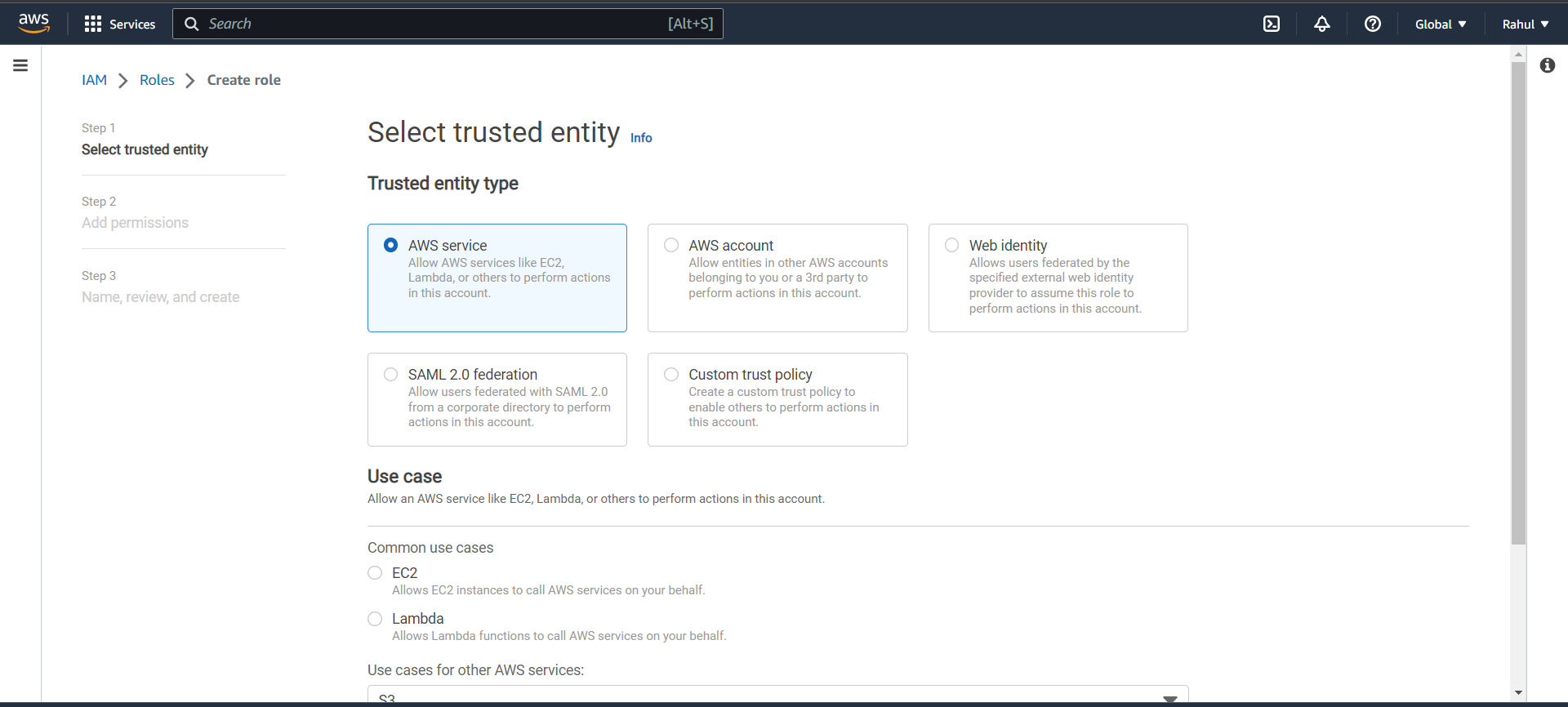
Step 12) Destination bucket will be created.



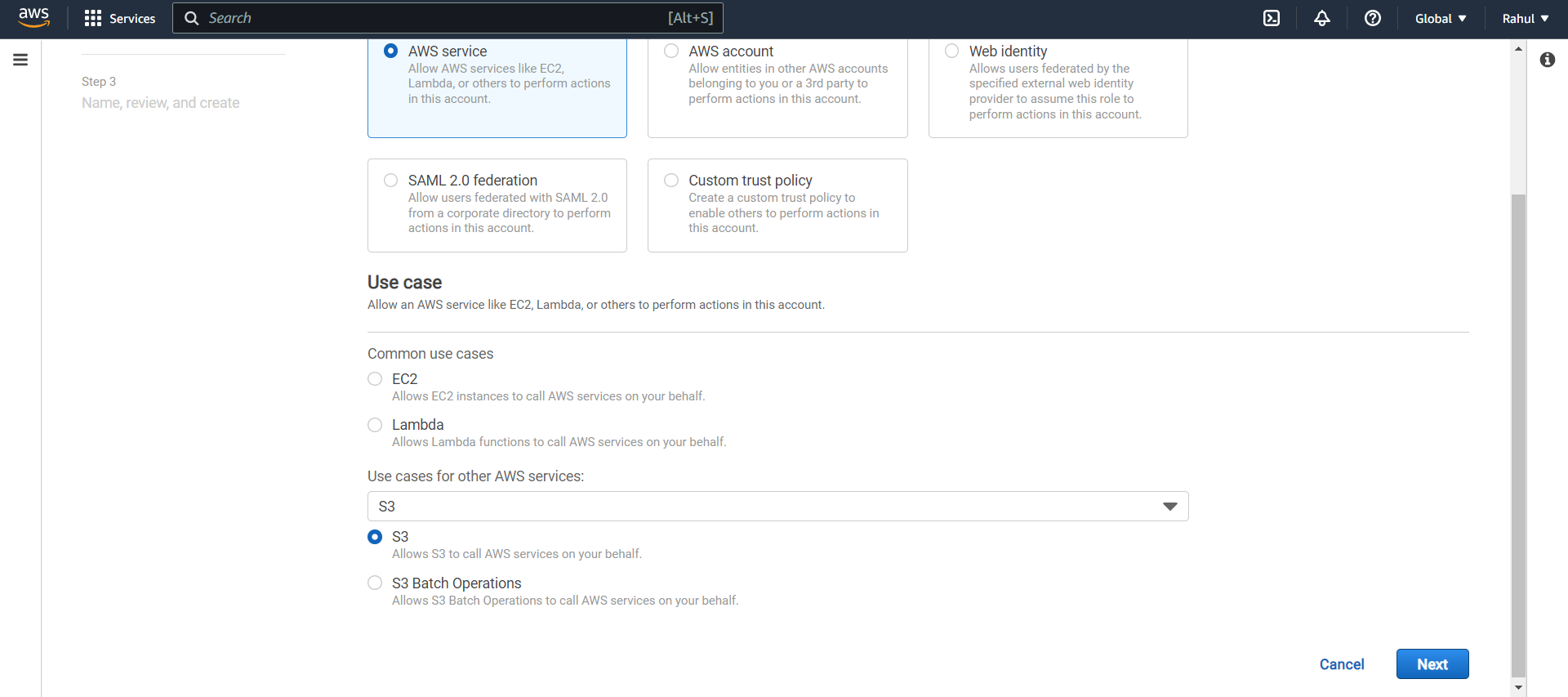
Step 13) Now, go to IAM -> Role -> Create Role.



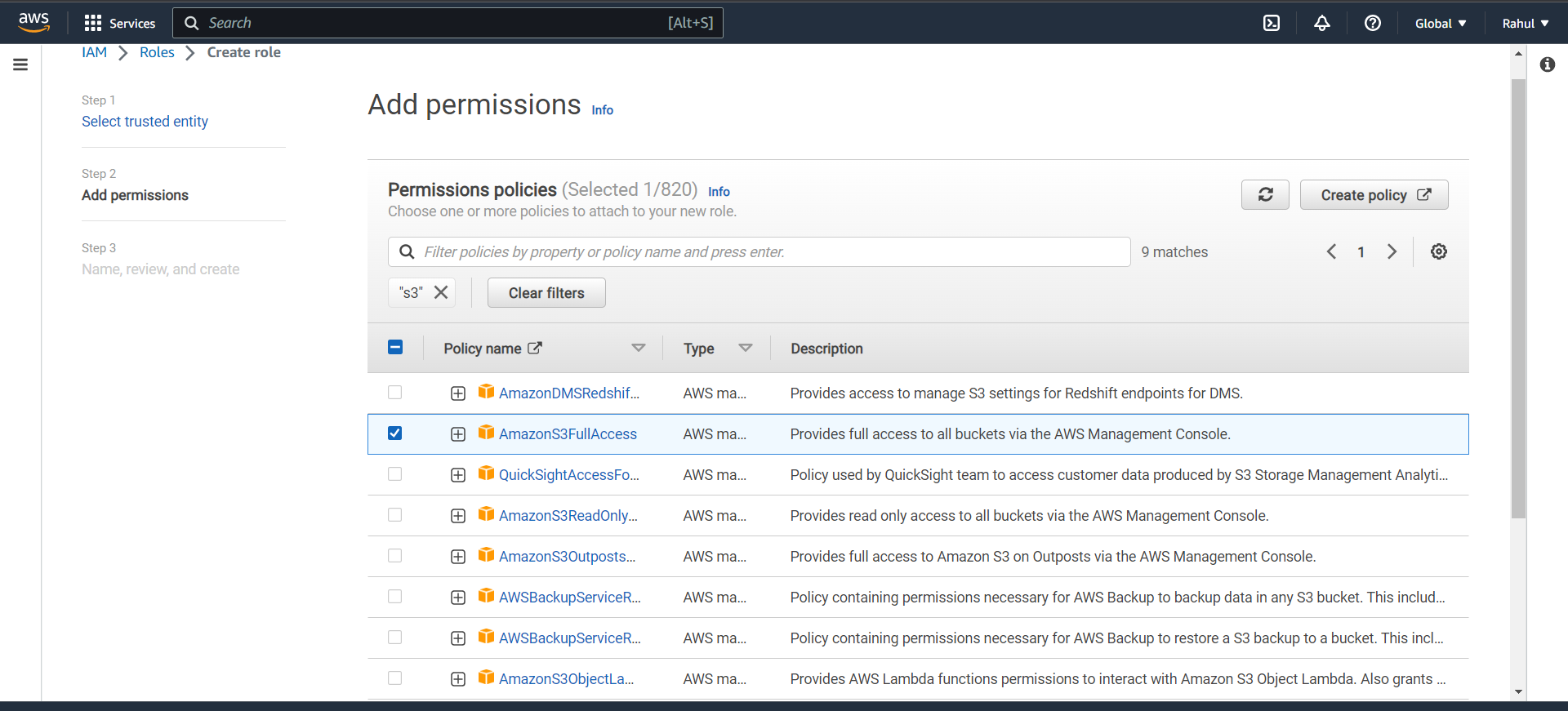
Step 14) Entity type – AWS Service.



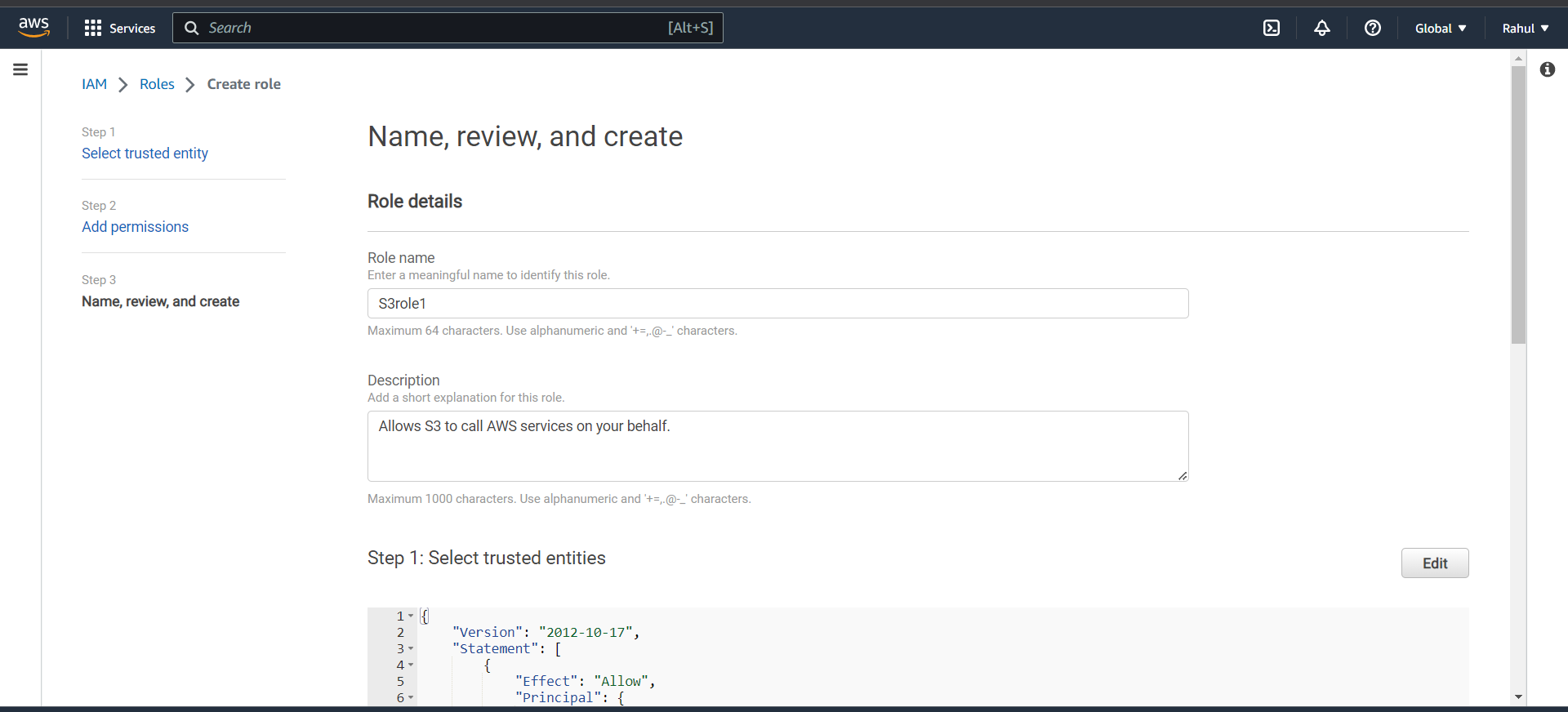
Step 15) Use case -> S3 and click on next.



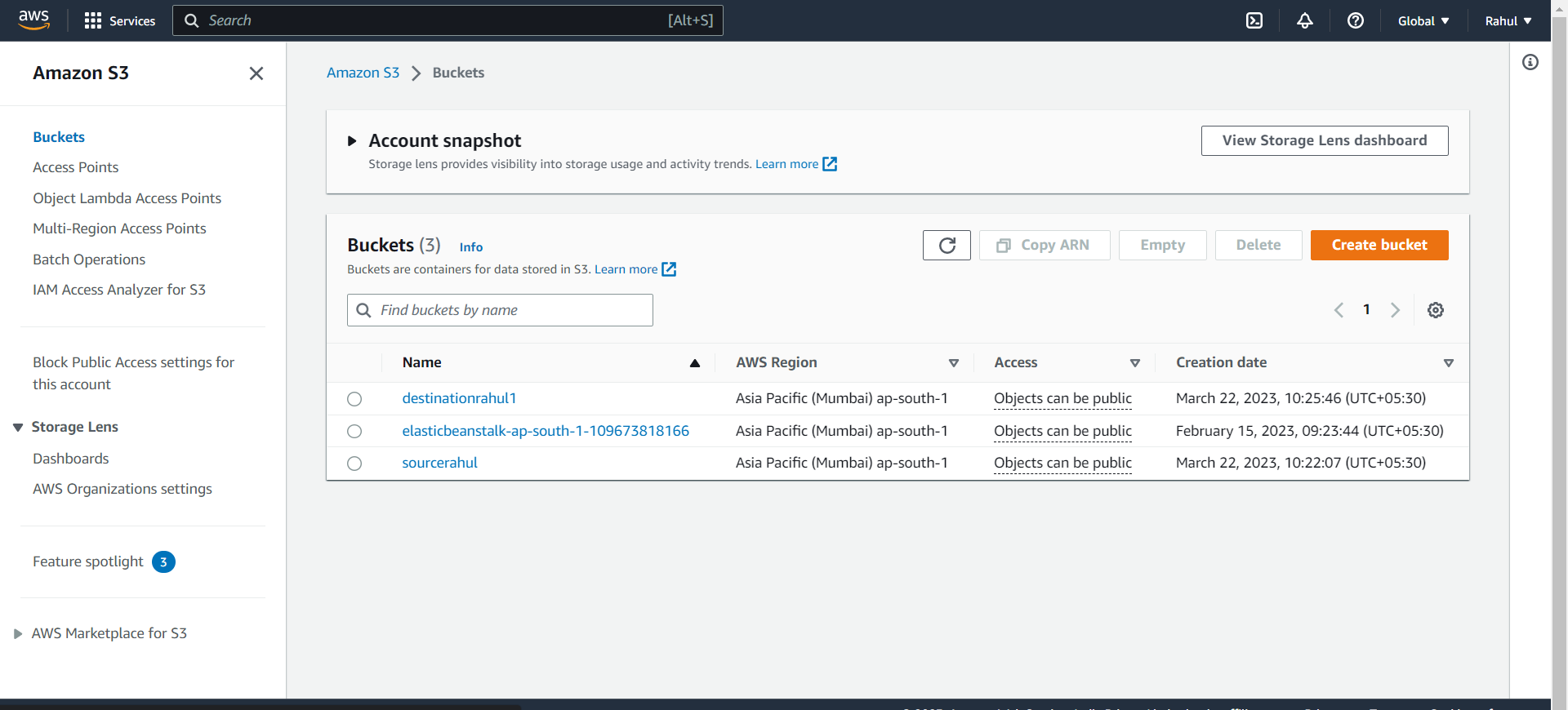
Step 16) Add permissions -> AWS S3 Full Access.



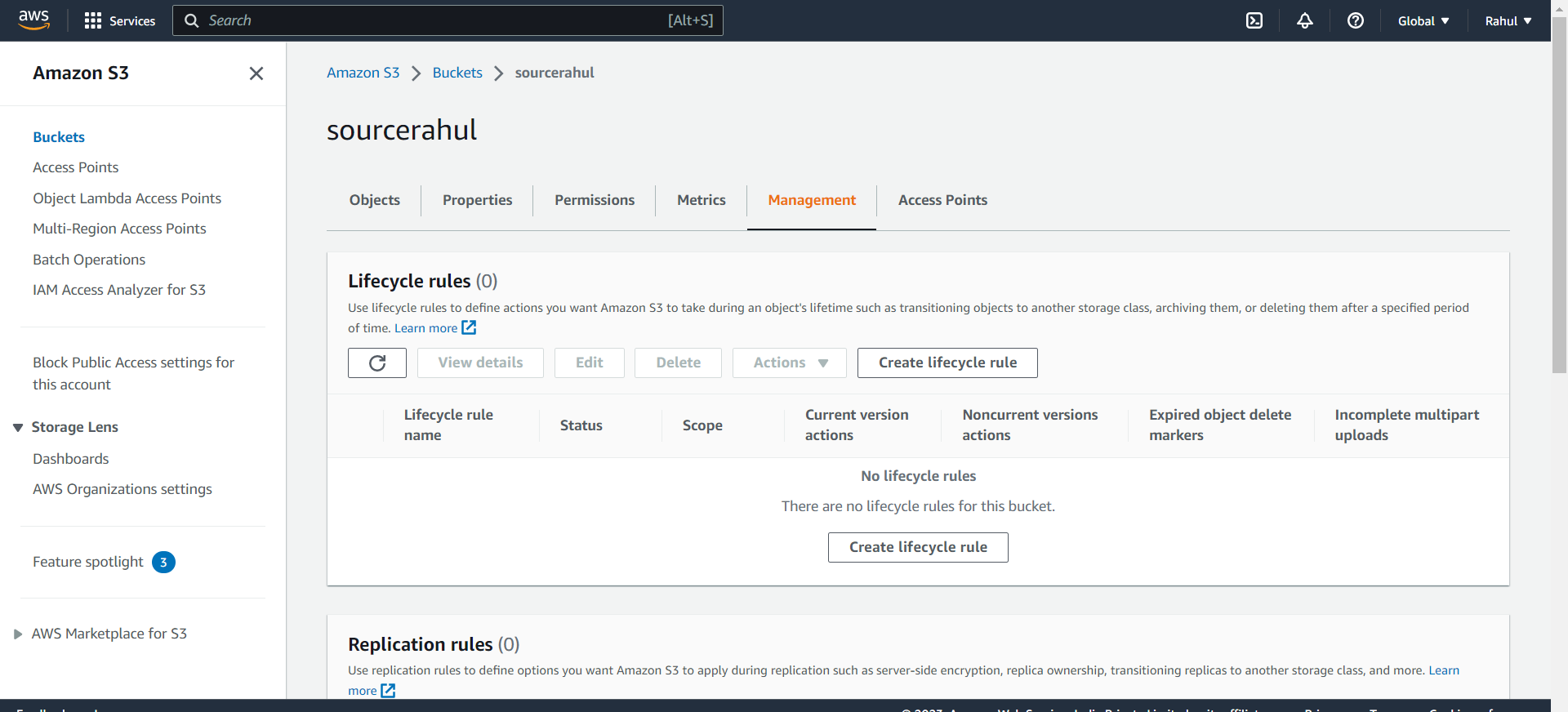
Step 17) Give it a name.



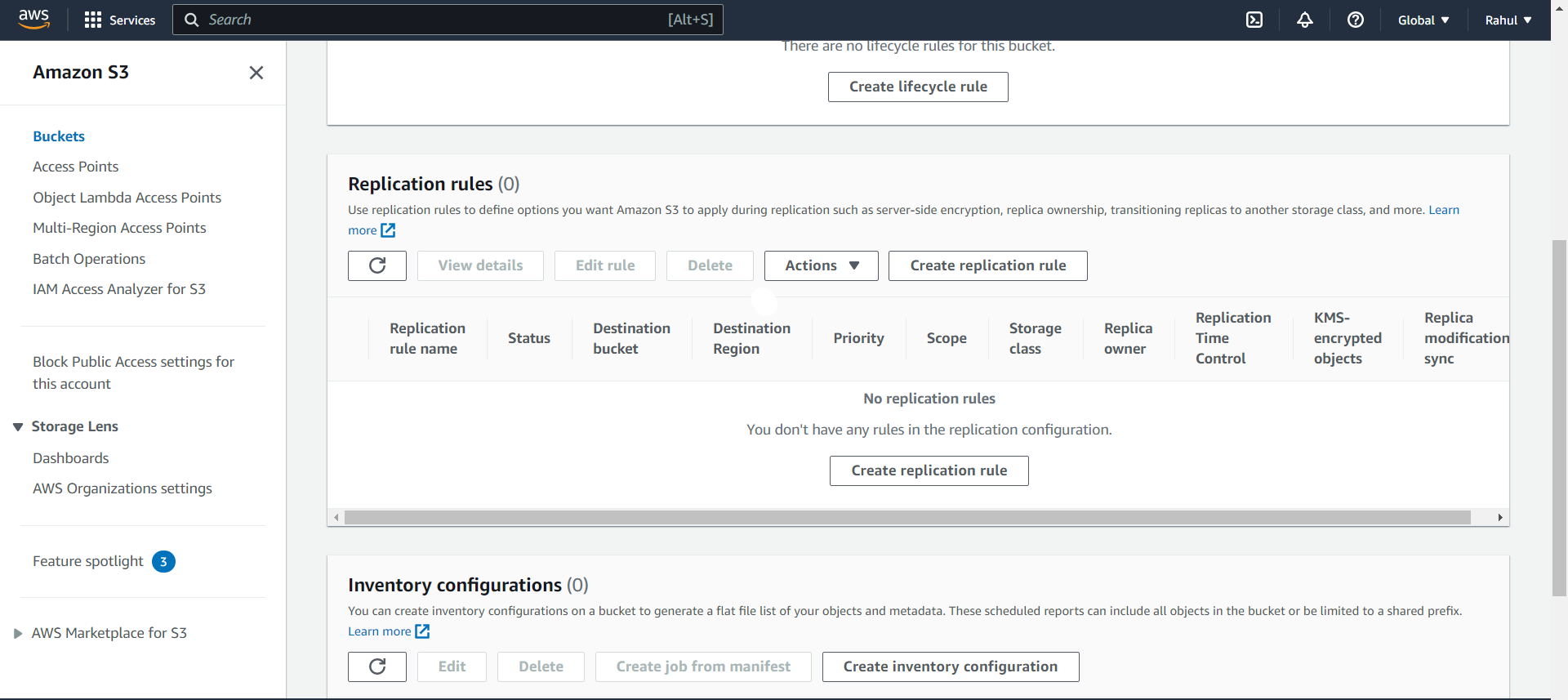
Step 18) Go back to S3, click on source bucket.



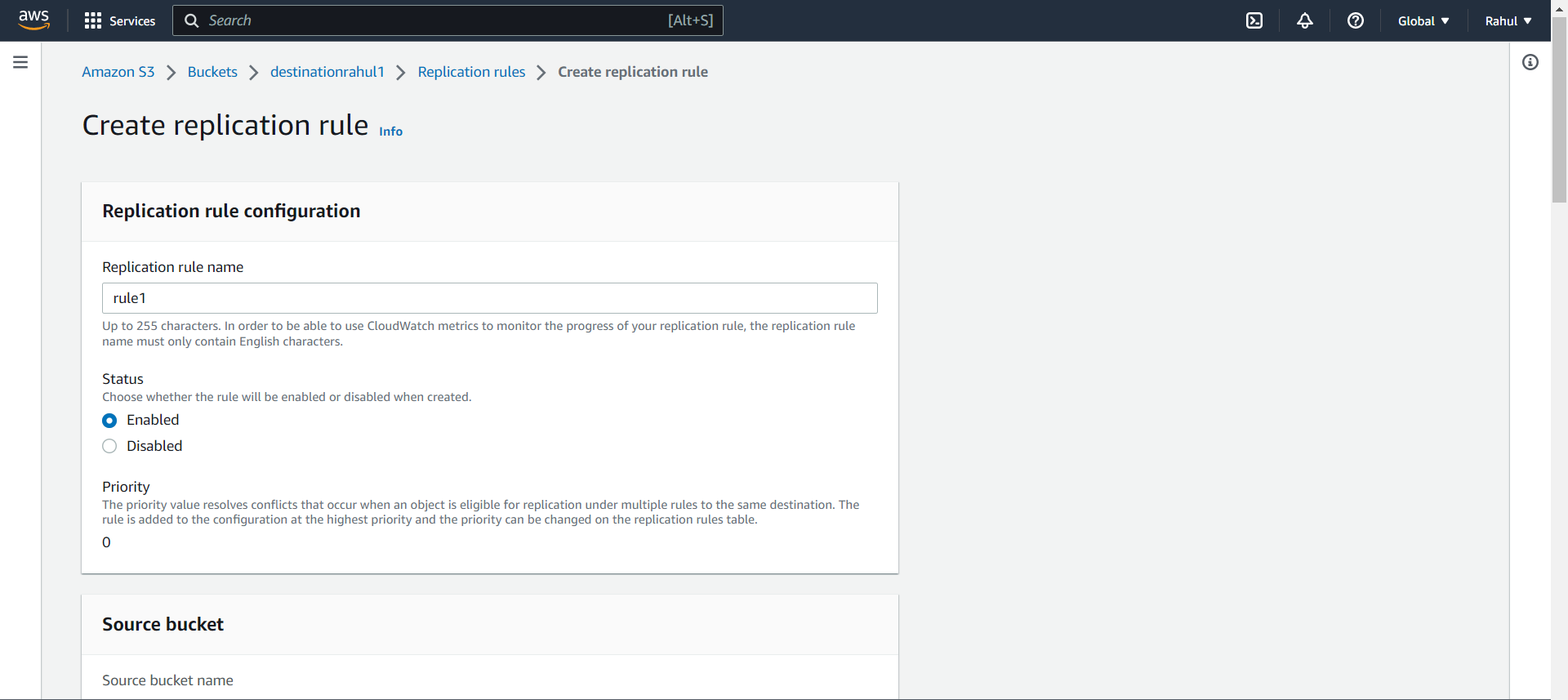
Step 19) Go to management.



Step 20) Replication rules -> create replication rule.

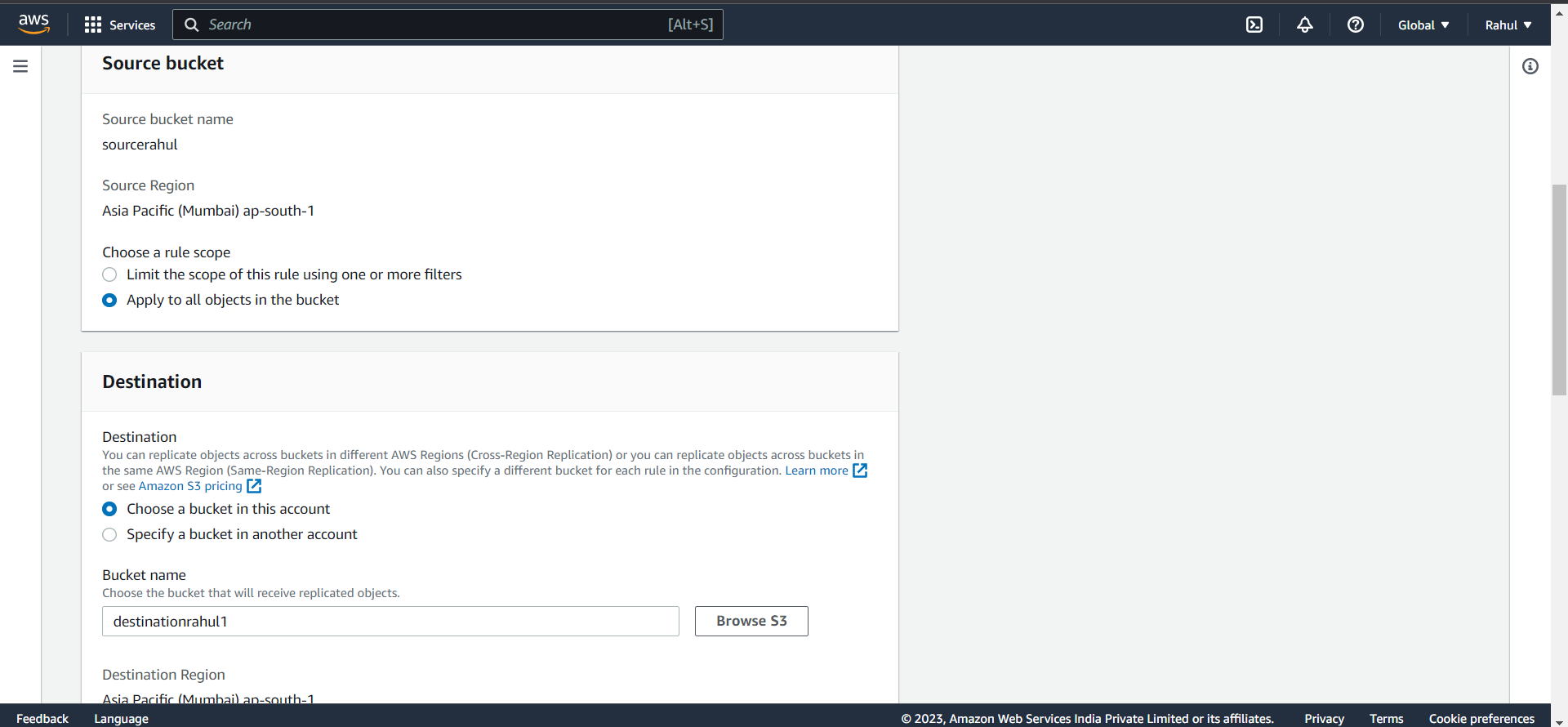


Step 21) Give it a name and status -> enabled.



Step 22) Under rule scope select -> Apply to all objects in bucket.

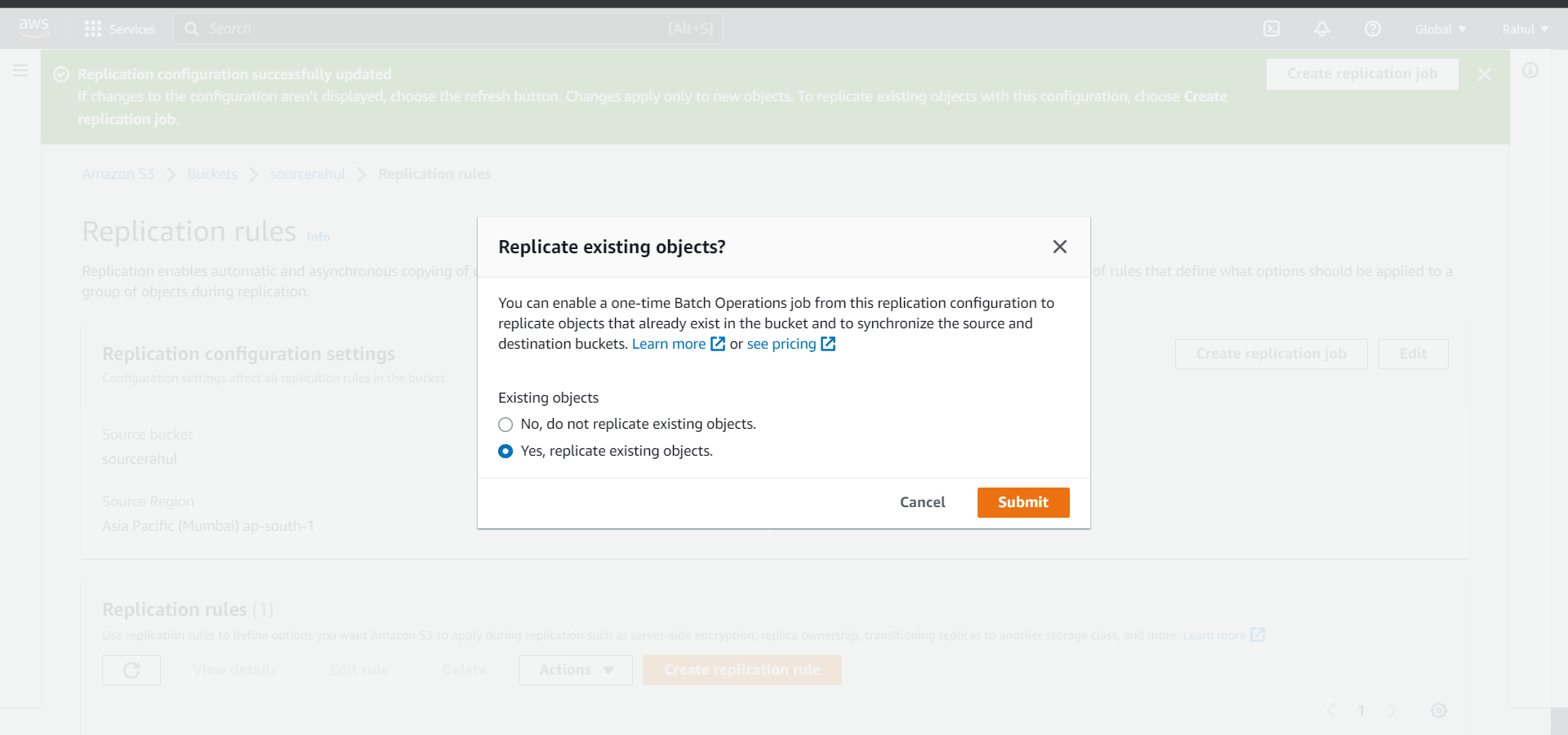
Under Destination browse and select destination bucket.



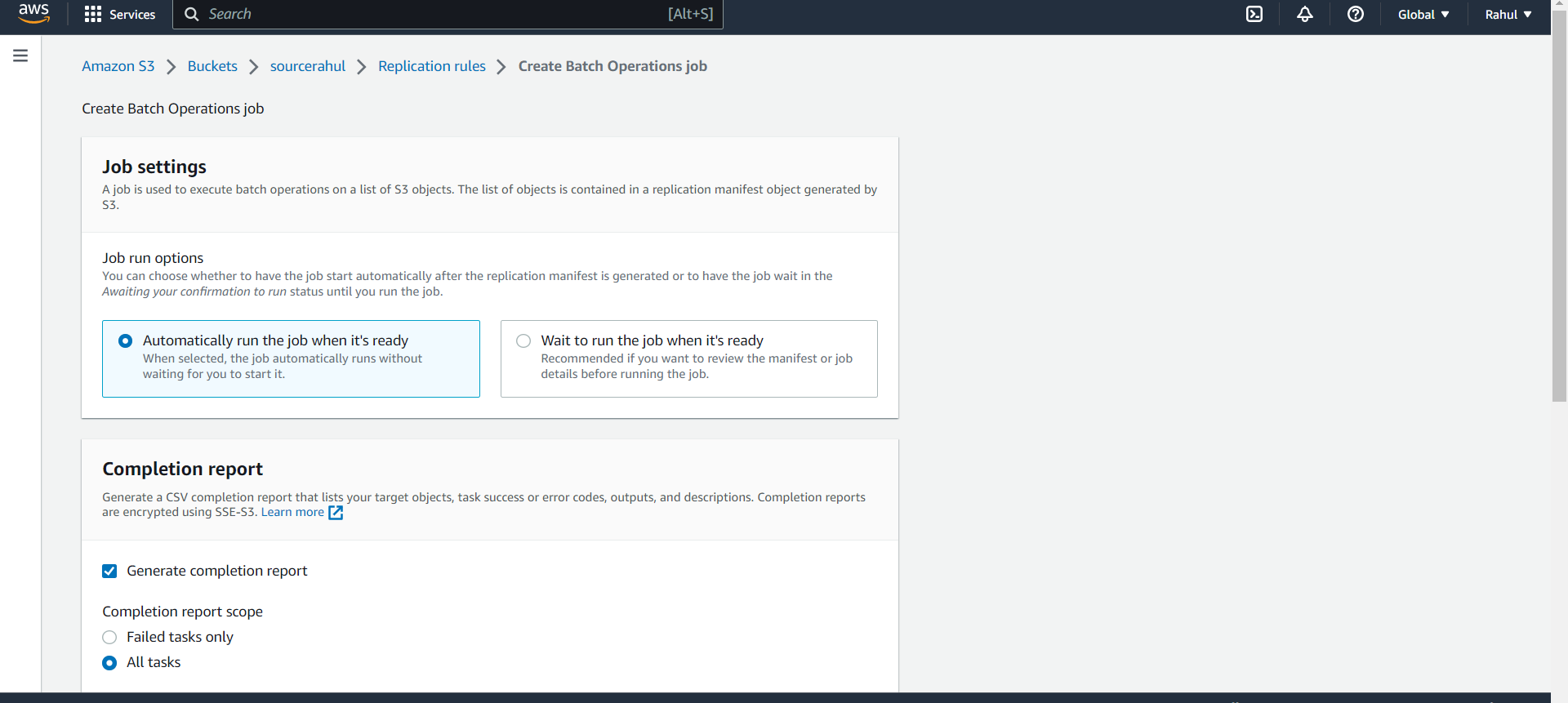
Step 23) Under IAM role select the role created.



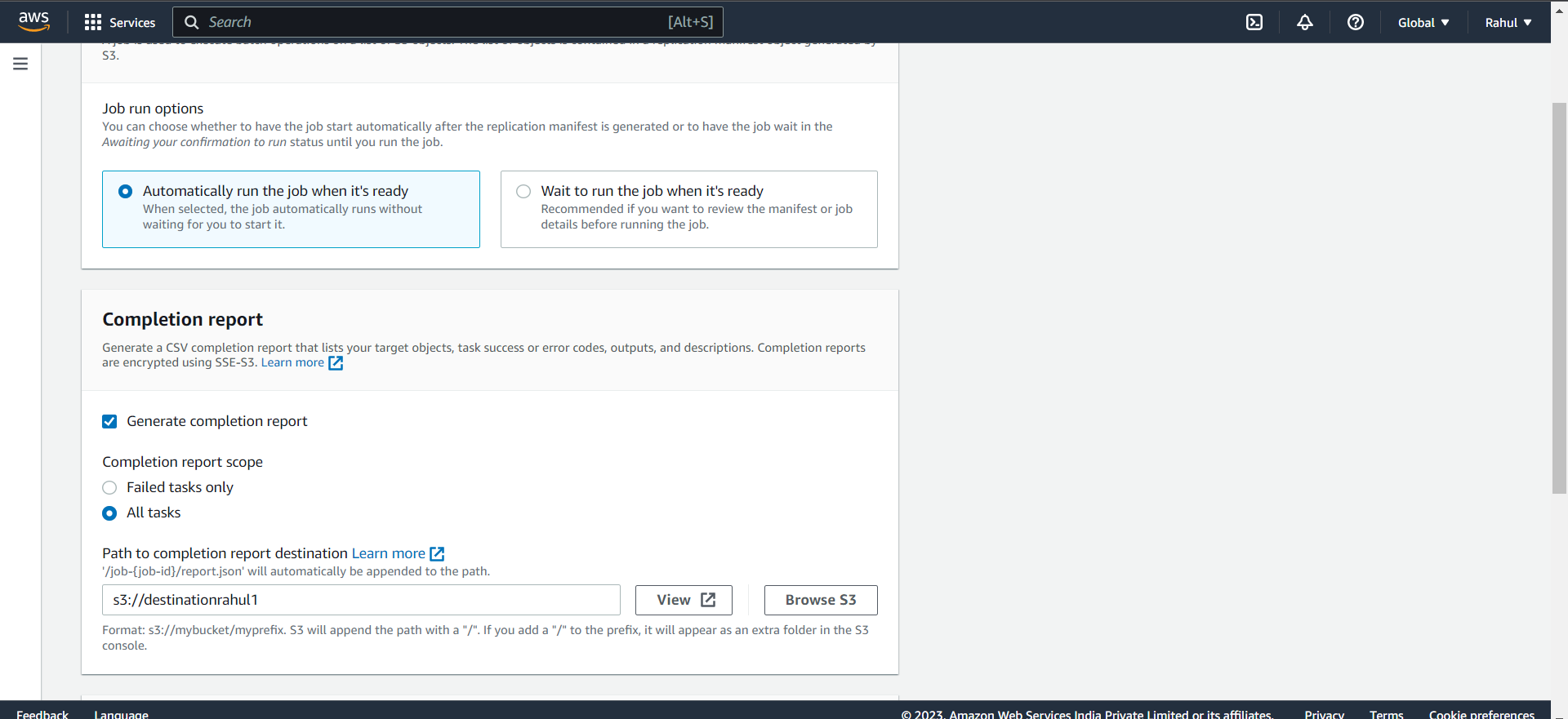
Step 24) Click next and select yes to replicate existing object.



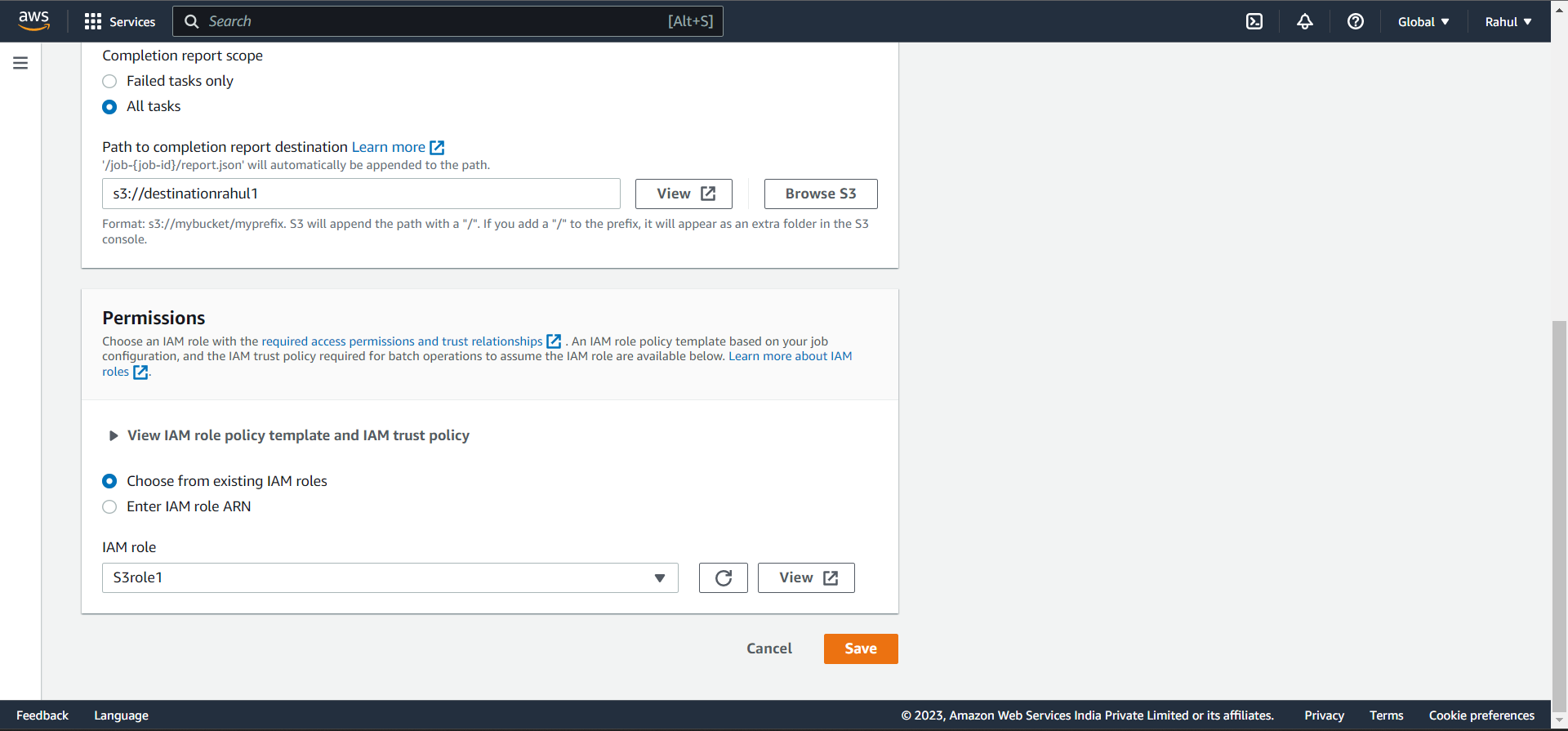
Step 25) Job settings -> automatically run the job when ready.



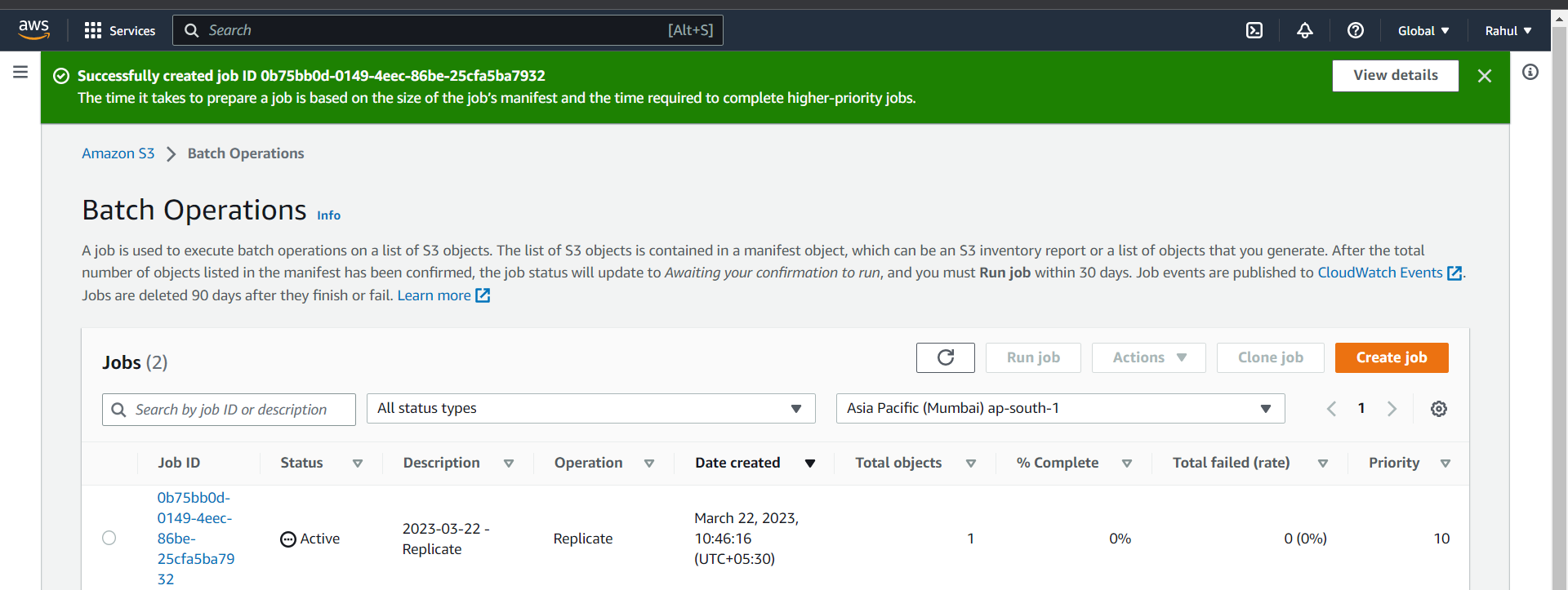
Step 26) Under Completion report, select Generate completion report and all tasks.



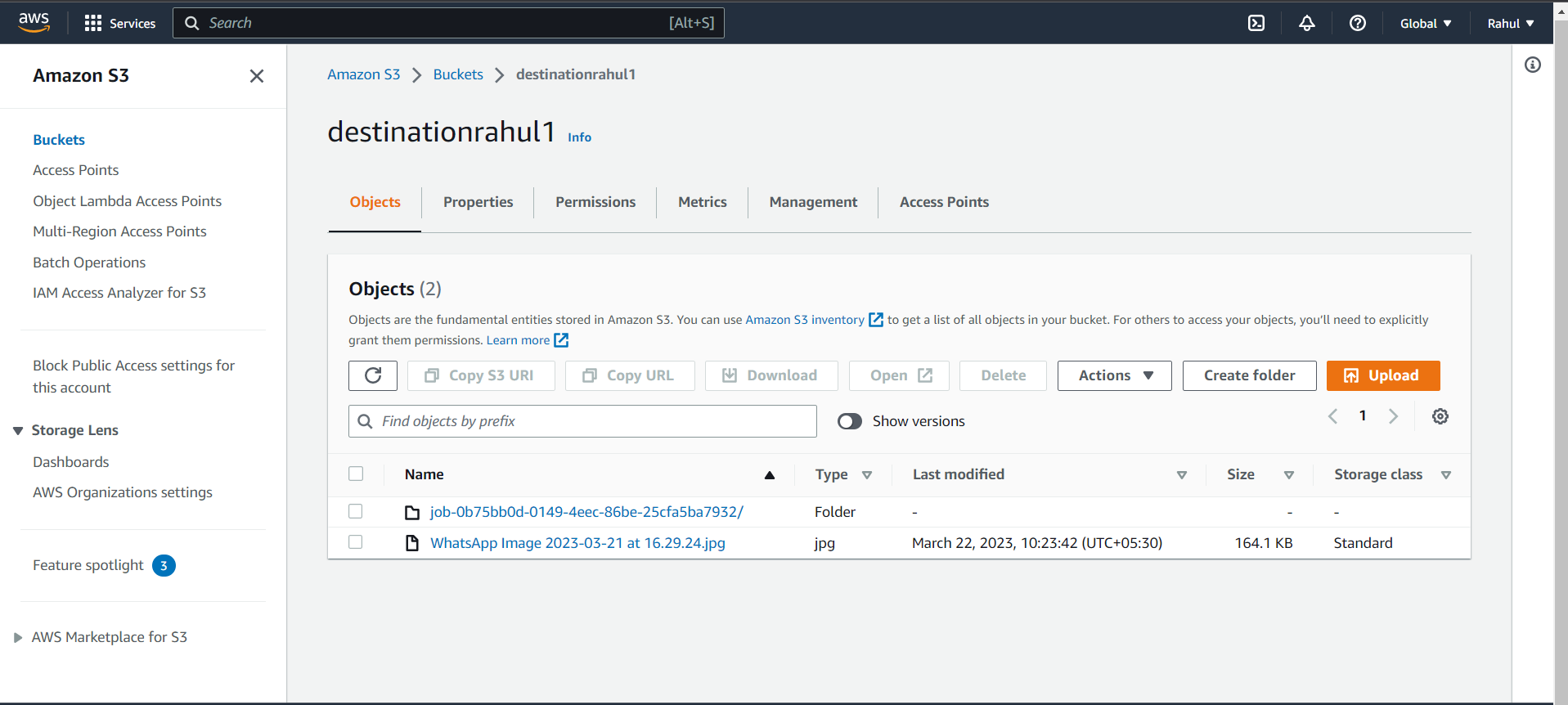
Step 27) Under permissions Choose IAM role created.

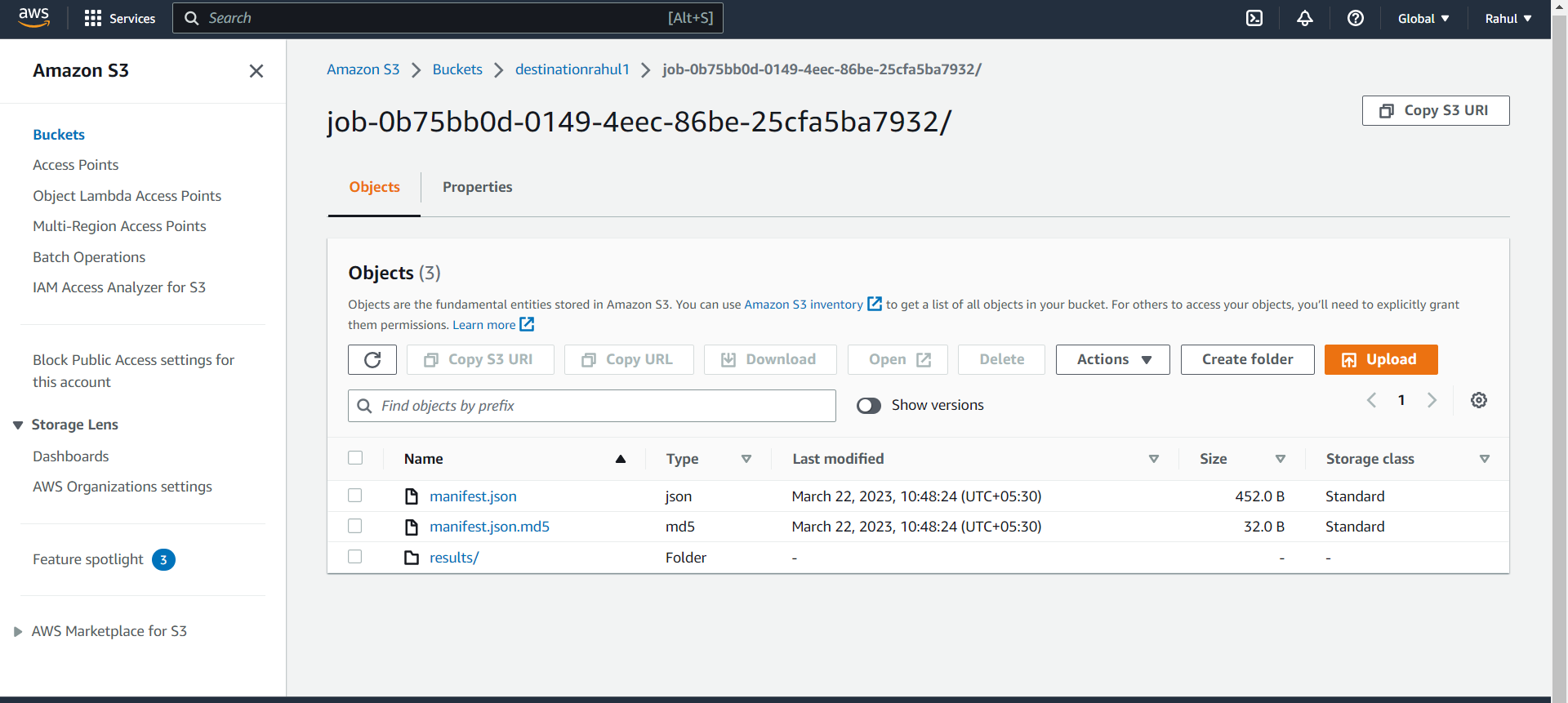


Step 28) The batch operation will take place.

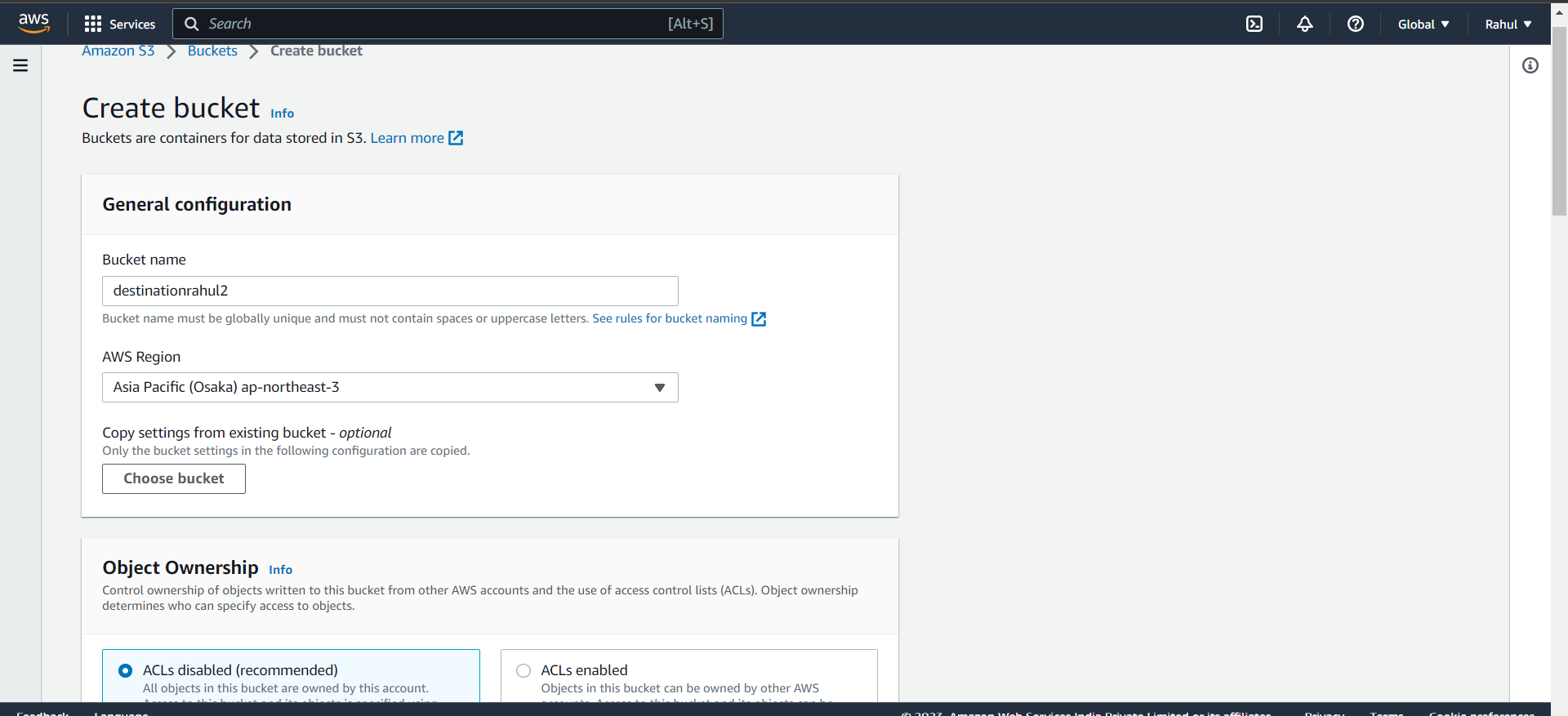


Step 29) After batch operation is completed, go to destination bucket and as we can see the replication has been performed.

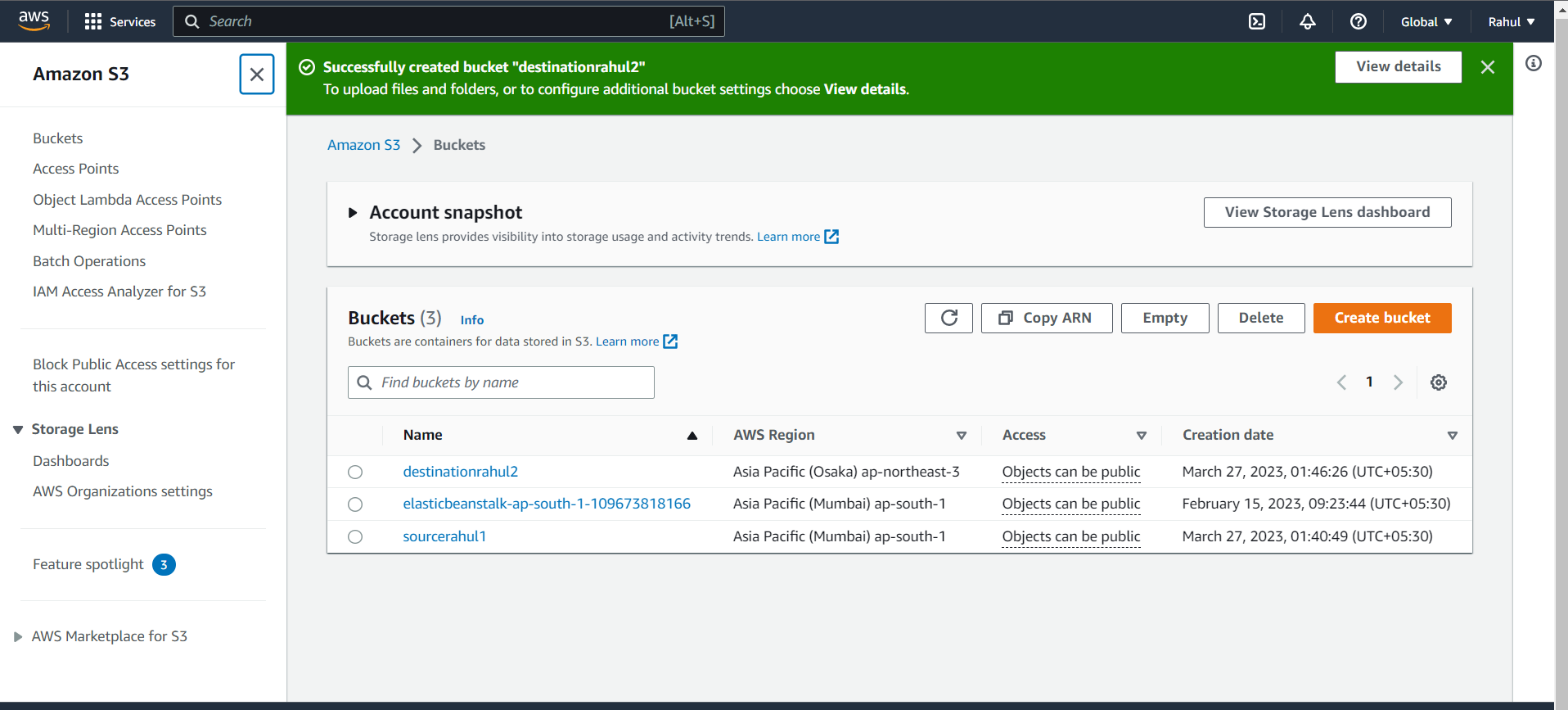


Step 30) Job report.

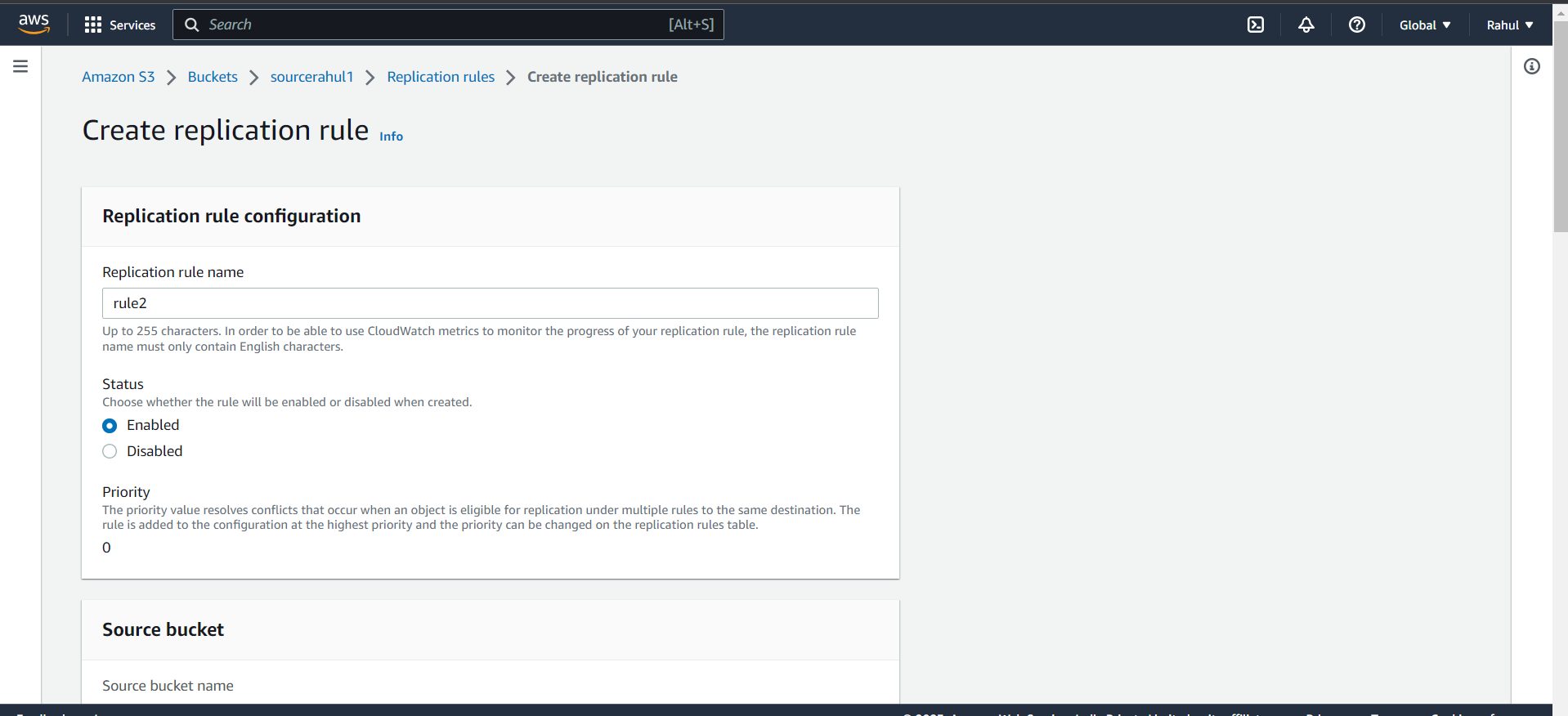
Step 31) Now for a different region, create another bucket in a different region.



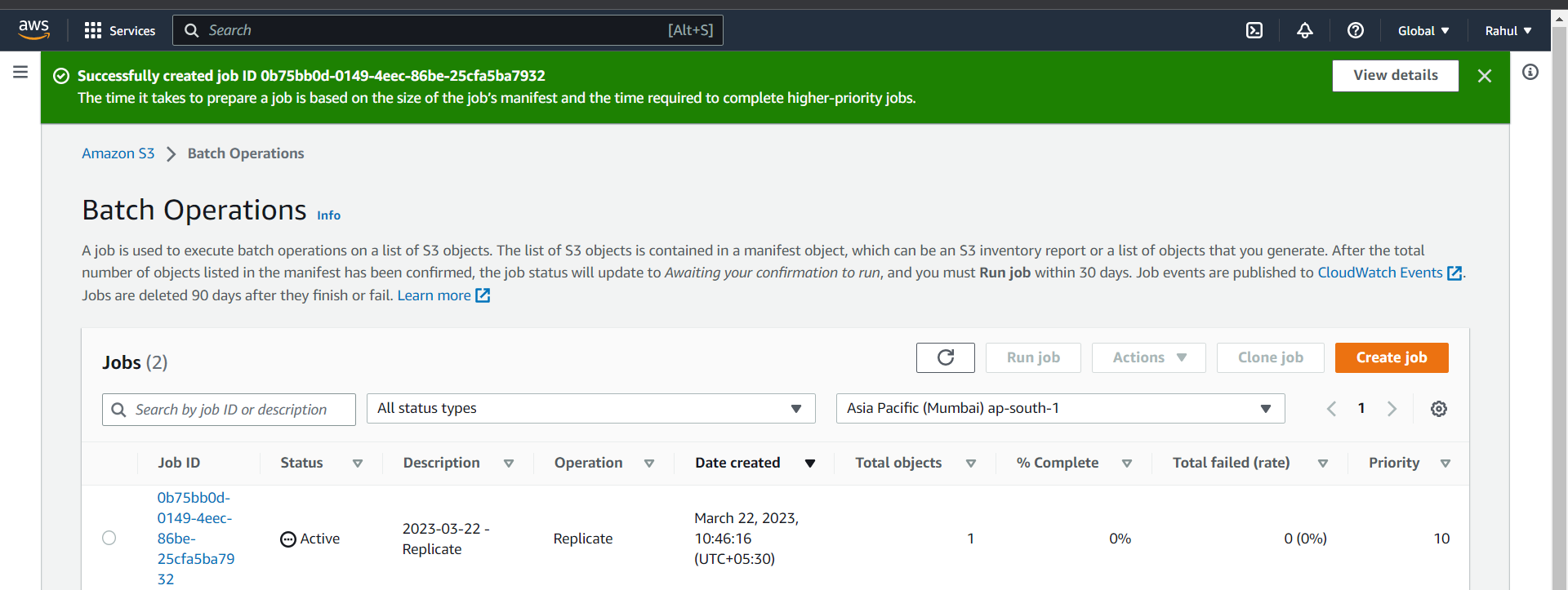
Step 32) As you can see we have created bucket in a different region.



Step 33) Again create replication rule in sourcebucket.

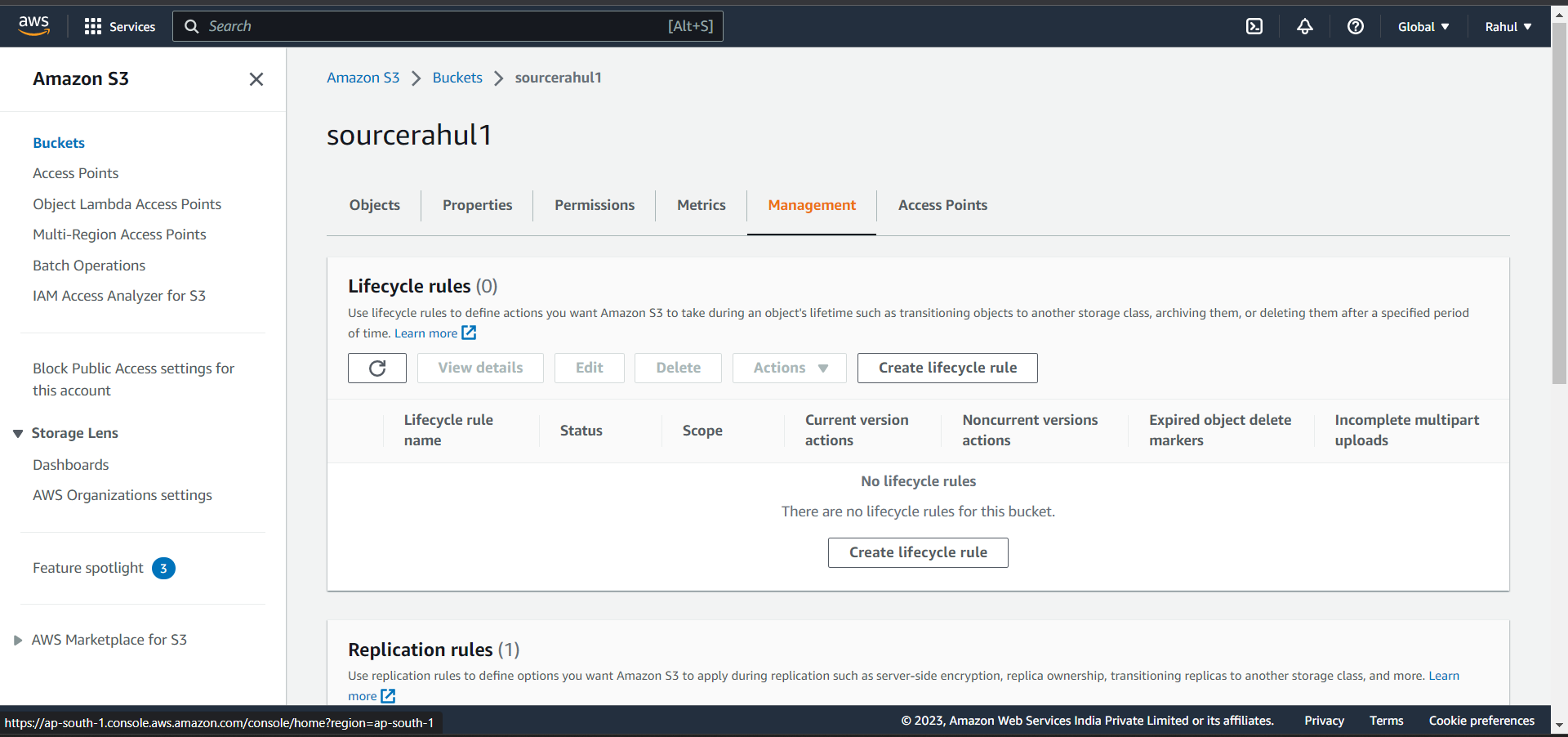


Step 34) Create the same replication rule.

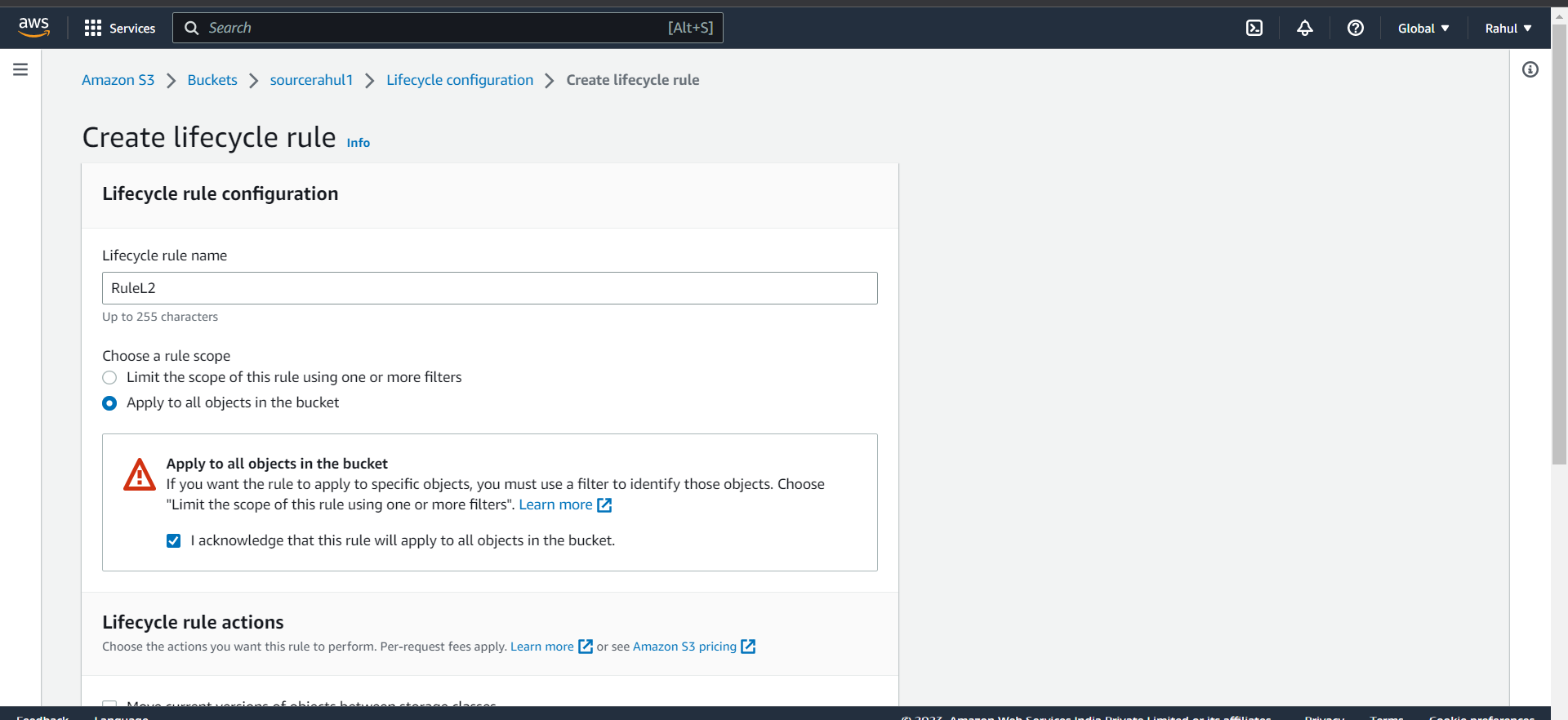


**ii) Delete the object through Lifecycle rule creation.**

Step 35) Go to Source bucket -> management -> Create lifecycle rule.

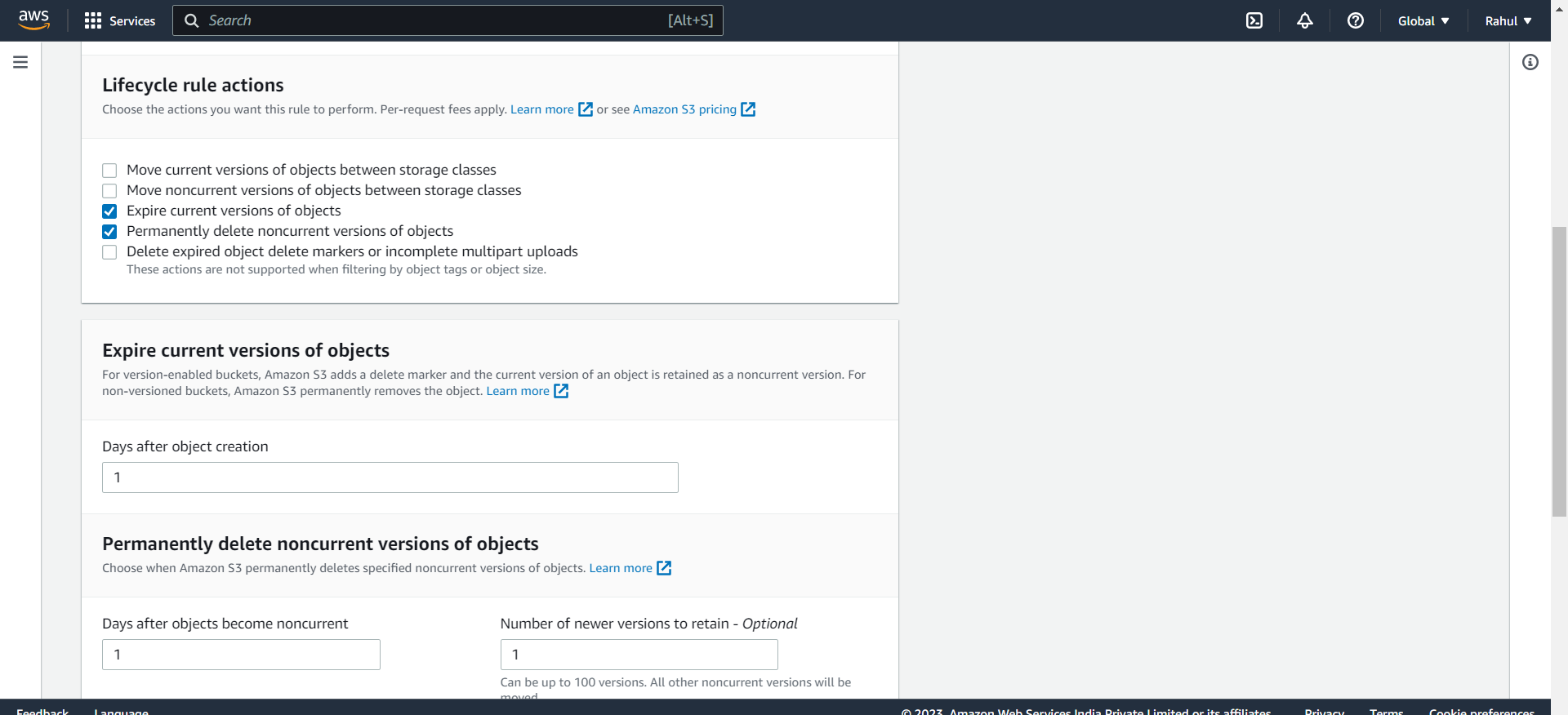


Step 36) Give the role a name, select Apply to all objects.

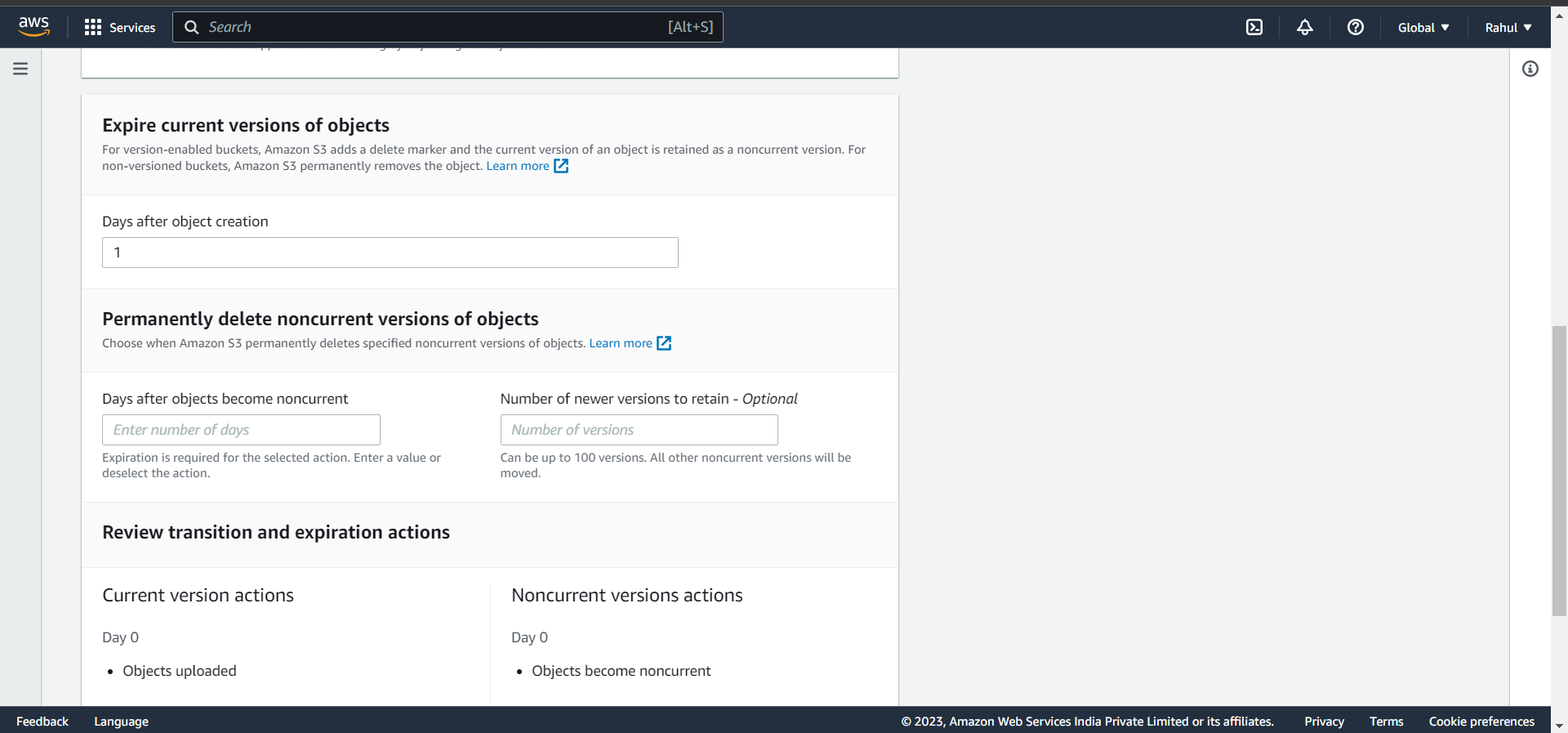


Step 37) Under Lifecycle rule actions select –

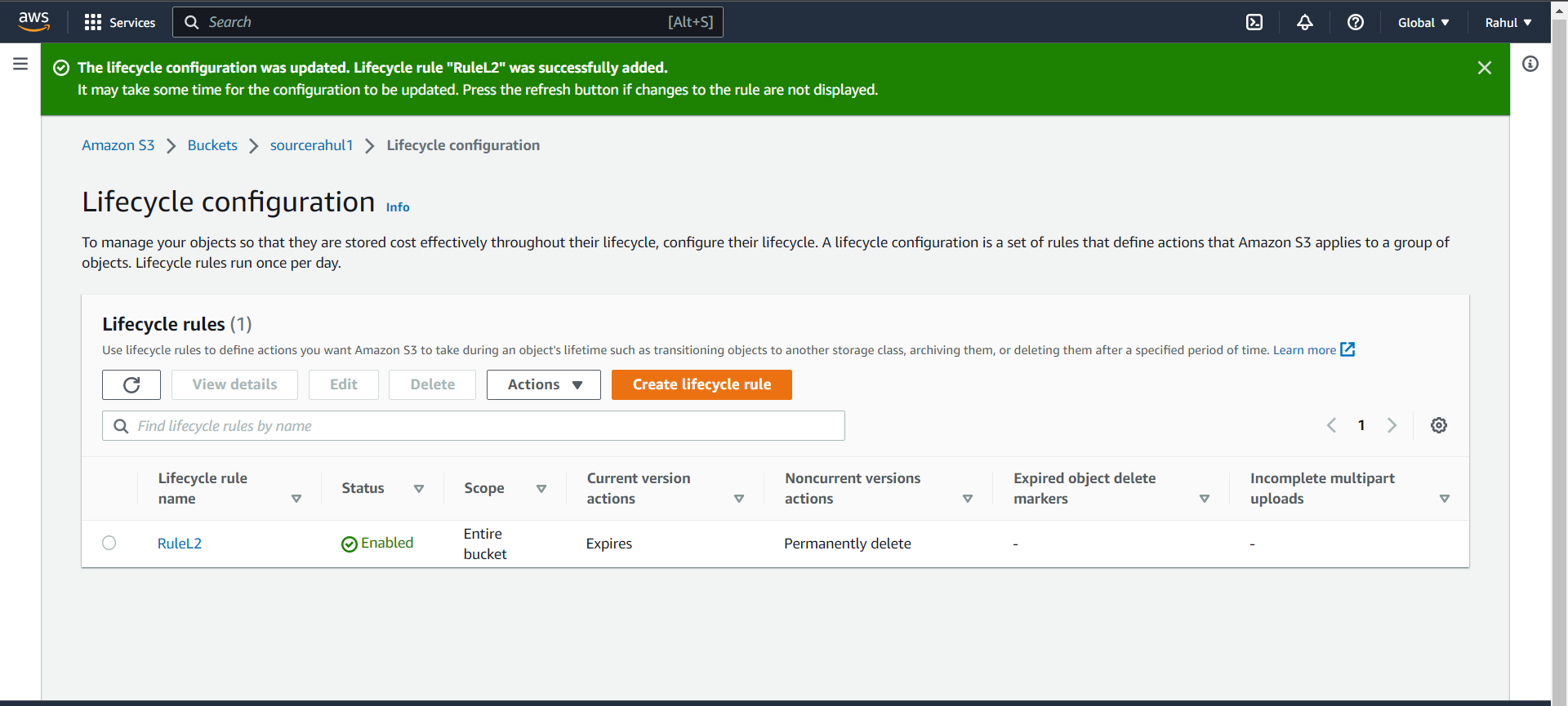
* Expire current versions of objects.
* Permanently delete noncurrent versions of objects.



Step 38) Select days after objects will delete.



Step 39) Rule created.



**iii) Create a transition action to move the object from one storage class to another.**

Step 40) Create another lifecycle rule.



Step 41) Under Lifecycle rule actions, select - Move current versions of objects between storage classes.



Step 42) Under Transition current versions of objects between storage classes,

Select storage class – Glacier instant retrieval, days and create rule.



Step 43) Rule created.

