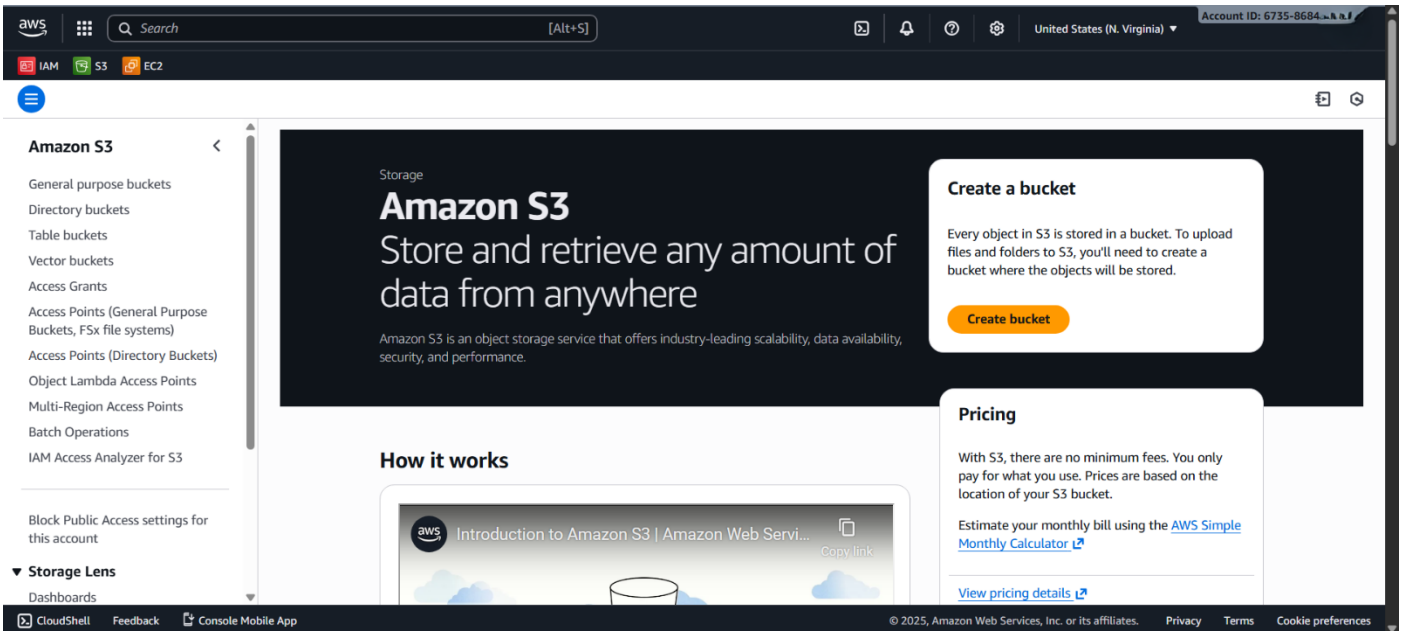
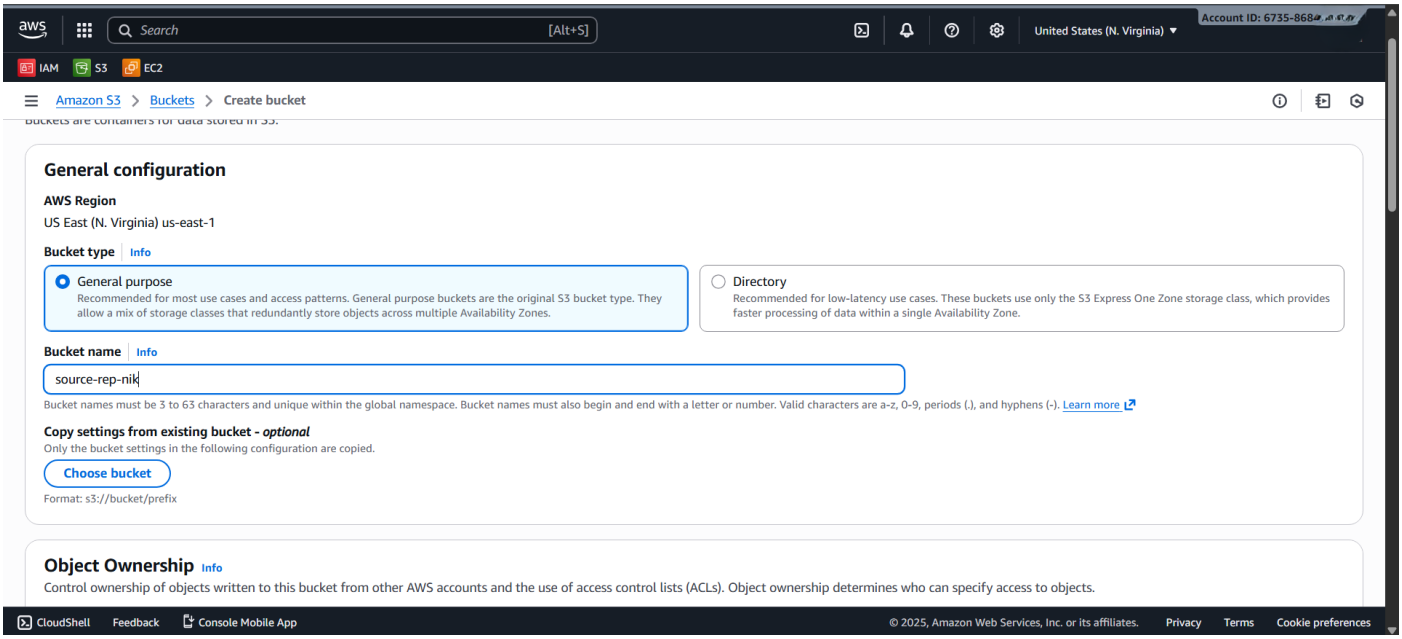
Create a S3 Bucket Replica from one AWS account to another AWS account

By: Nikhilesh Sakhare

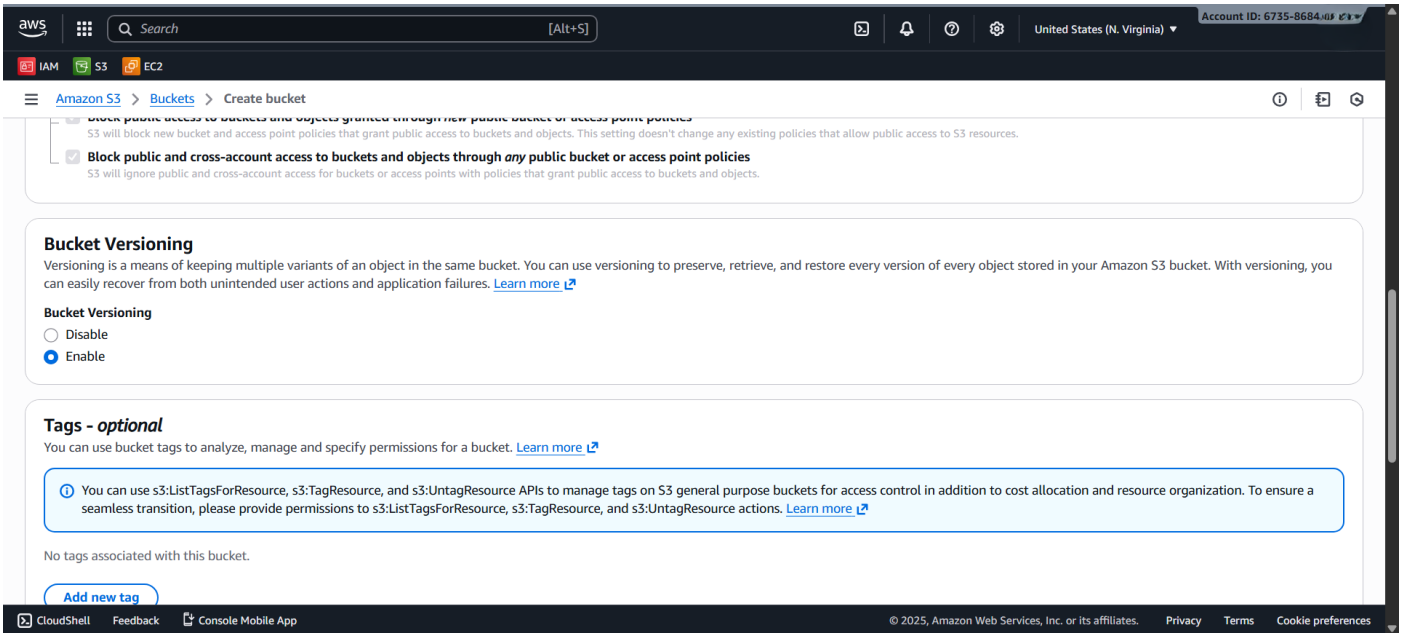
1. Sign in to the AWS Management Console with credentials for the sourse AWS account (Account A) and open the Amazon S3 service home page.



2. Click Create bucket, select General purpose as the bucket type, choose region US East (N. Virginia) us-east-1, and enter a unique bucket name such as source-rep-nik, then leave block public access enabled and complete the creation.

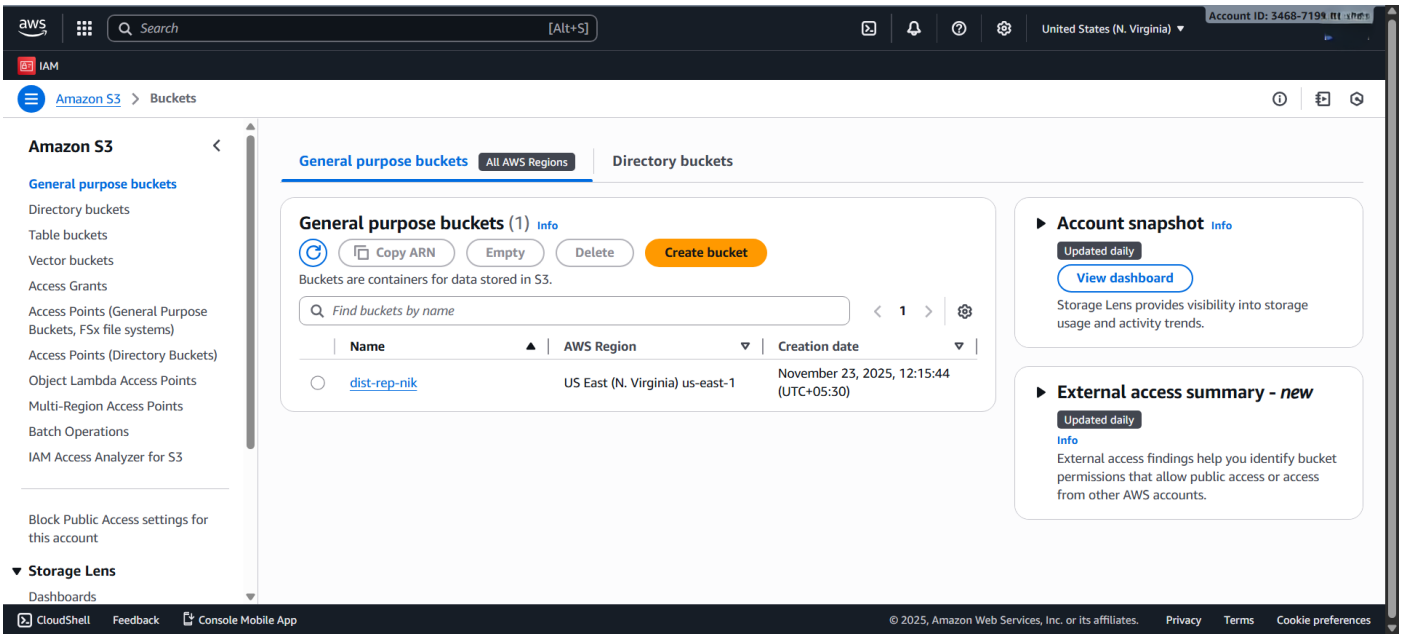


3. Scroll down in the bucket-creation form and enable Bucket Versioning, which is required for replication, then create the bucket.

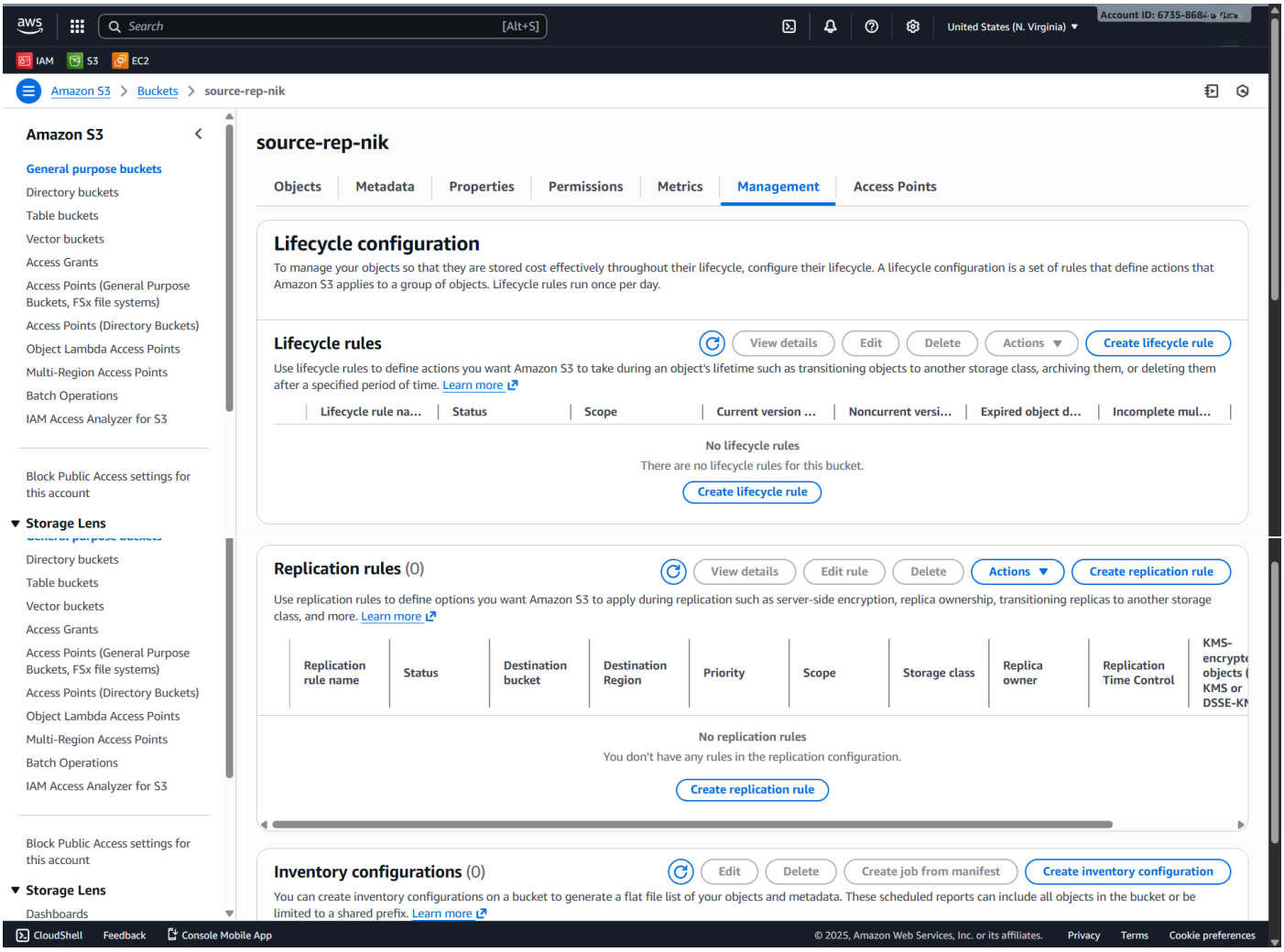


On the S3 console in Account A, the new source-rep-nik bucket now appears in the buckets list.

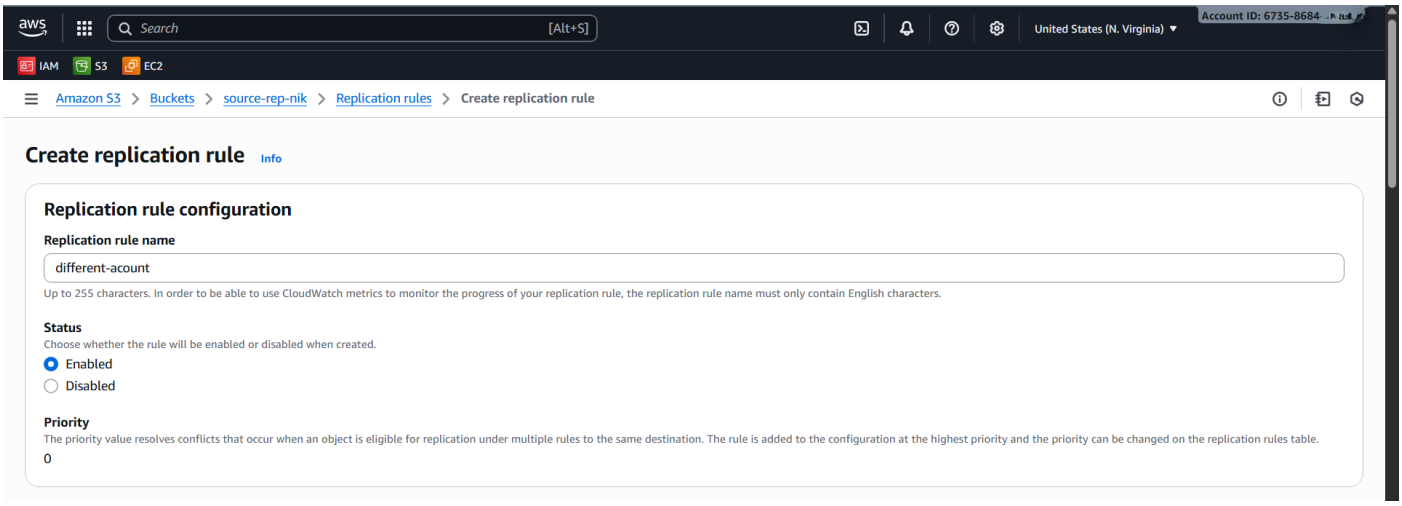
4. Switch to the source AWS account (Account B), open Amazon S3, and again click Create bucket. Use region US East (N. Virginia) us-east-1 and specify a bucket name such as dist-rep-nik; keep the type as General purpose.



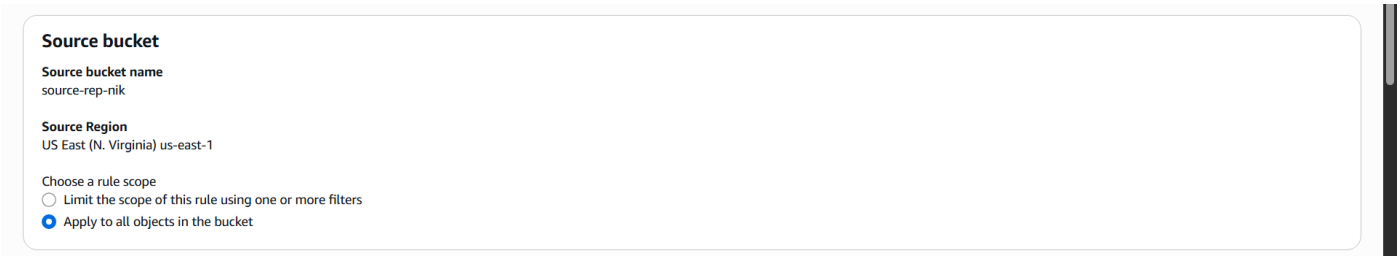
5. Open the source-rep-nik bucket in Account A and choose the Management tab, where the Replication rules section initially shows “No replication rules”. Click Create replication rule to start configuring cross-account replication for this bucket.



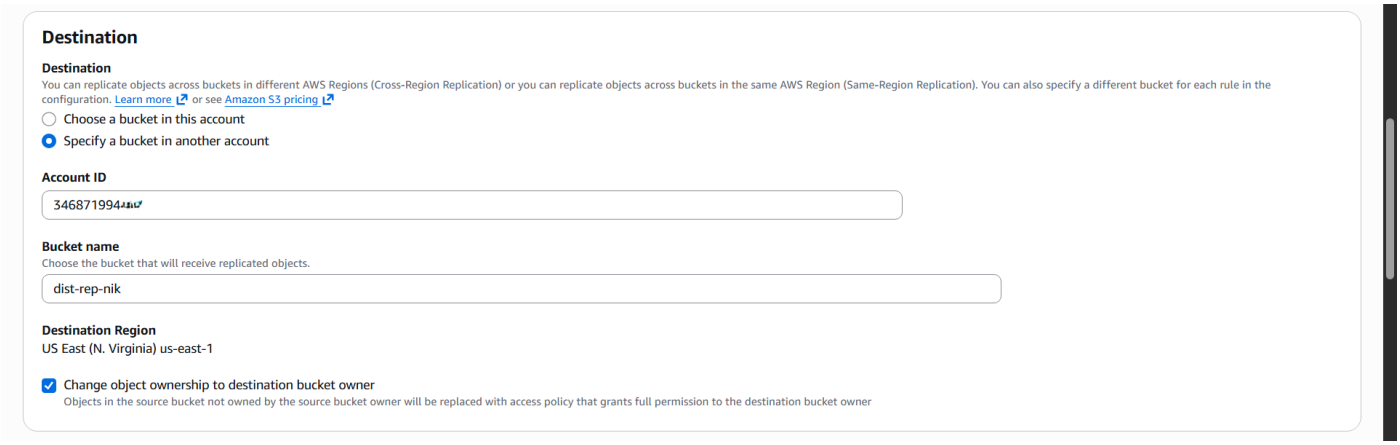
6. On the Create replication rule page, enter a rule name such as different-acount, set Status to Enabled, and leave Priority at 0.



7. Under Source bucket, confirm the bucket name source-rep-nik and choose Apply to all objects in the bucket so every object will be replicated.

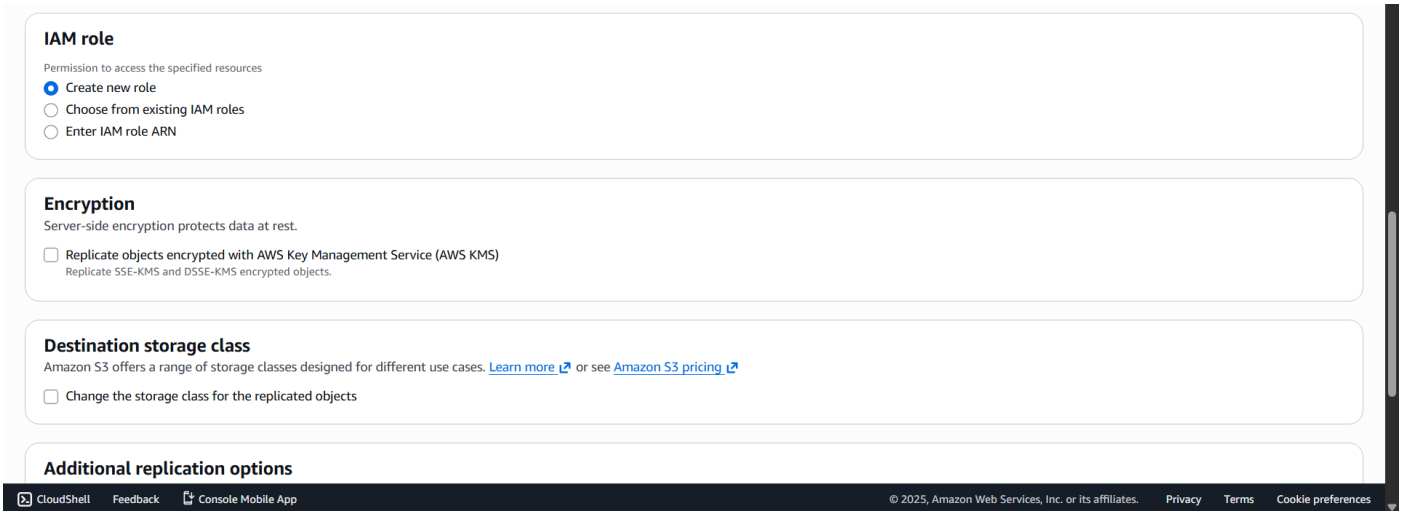


8. In the Destination section of the same rule wizard, select Specify a bucket in another account. Enter the Account ID of the destination account (e.g., 346871994407) and type the previously created destination bucket name dist-rep-nik; the Destination Region remains US East (N. Virginia) us-east-1.



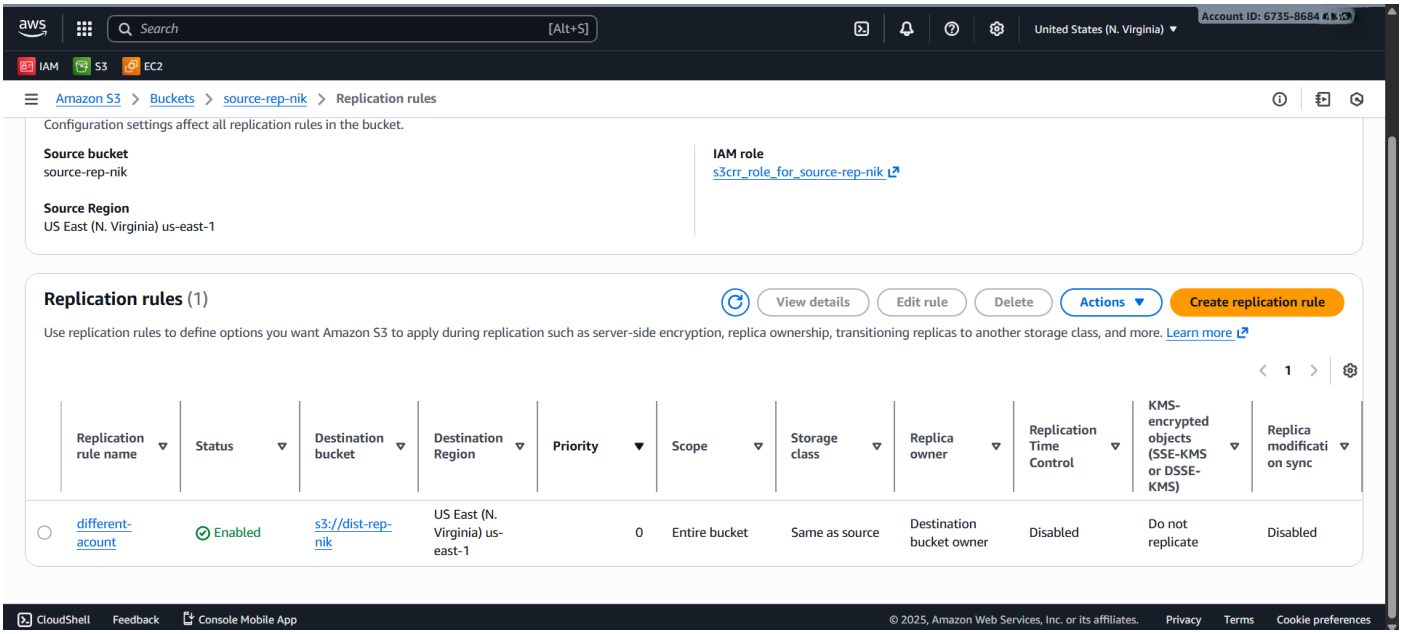
Check the option Change object ownership to destination bucket owner so that replicated objects are owned and fully manageable by Account B's bucket owner.

9. In the IAM role section of the replication rule, choose Create new role so Amazon S3 automatically creates a role that it will assume to perform replication.



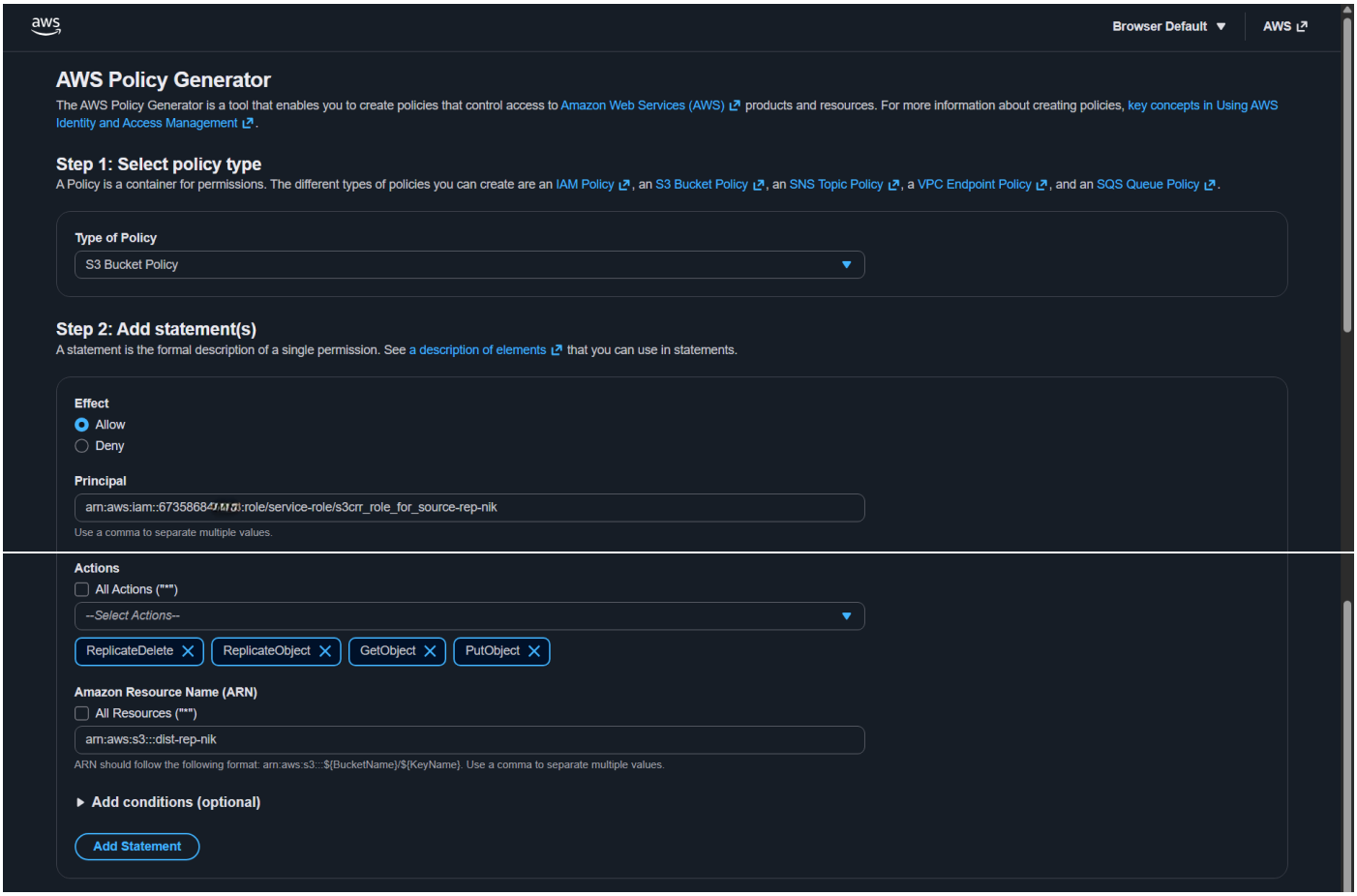
After the rule is saved, S3 creates a service role with a name like s3crr_role_for_source-rep-nik that has permission to read from the source bucket and write to the destination bucket.

10. Once all settings are reviewed, scroll to the bottom and click Save to create and enable the replication rule. Verify that the rule different-acount is listed with Status: Enabled, destination bucket s3://dist-rep-nik, region us-east-1, scope Entire bucket, and replica owner set to Destination bucket owner. The IAM role column links to the auto-created role s3crr_role_for_source-rep-nik, confirming that S3 has everything required to perform replication.

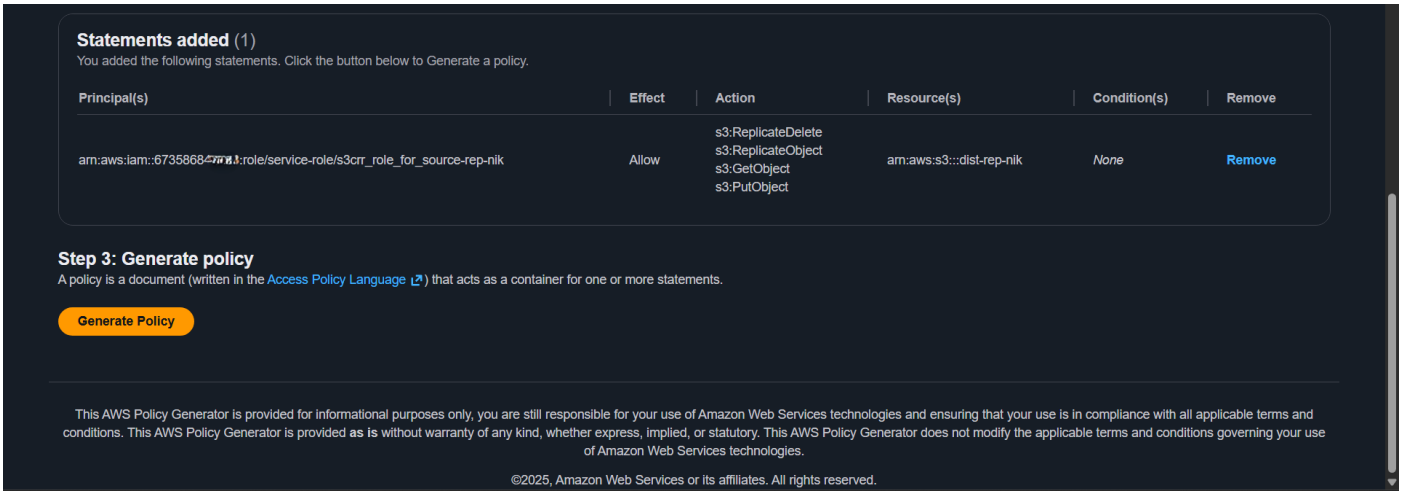


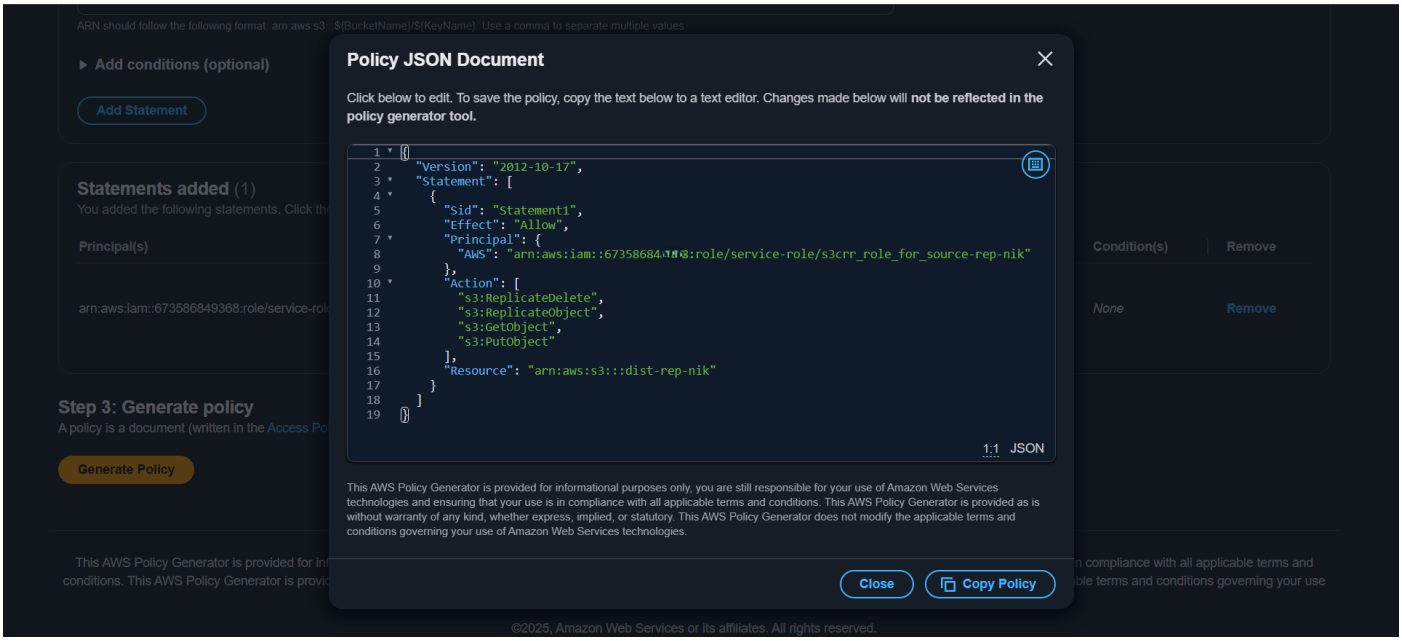
11. To allow the S3 replication role from Account A to write into dist-rep-nik, open a new browser tab with the AWS Policy Generator set to S3 Bucket Policy.

Configure the statement with:

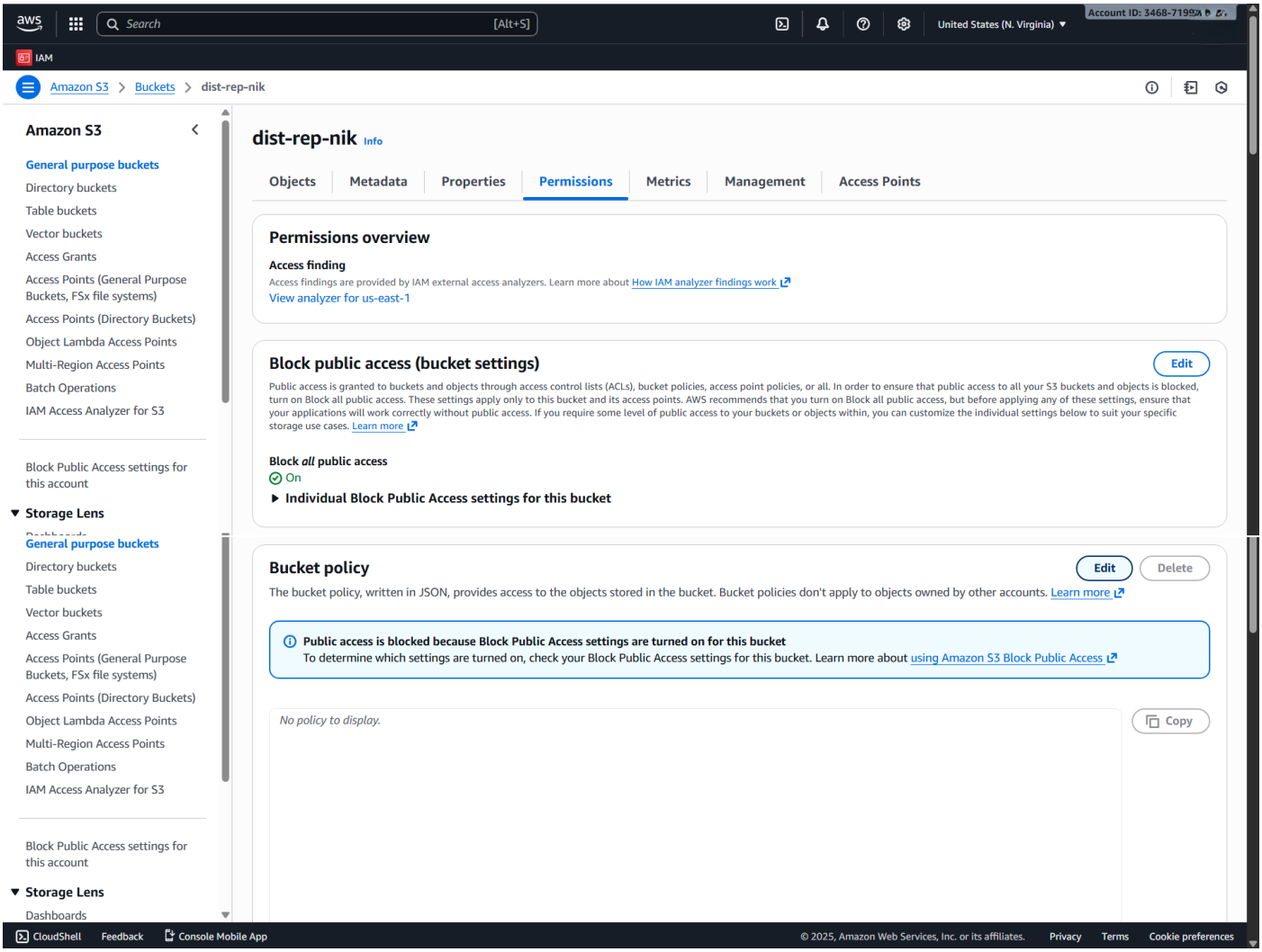


12. Click Add Statement and then Generate Policy to view the JSON document, which looks like this in the Policy Generator preview.

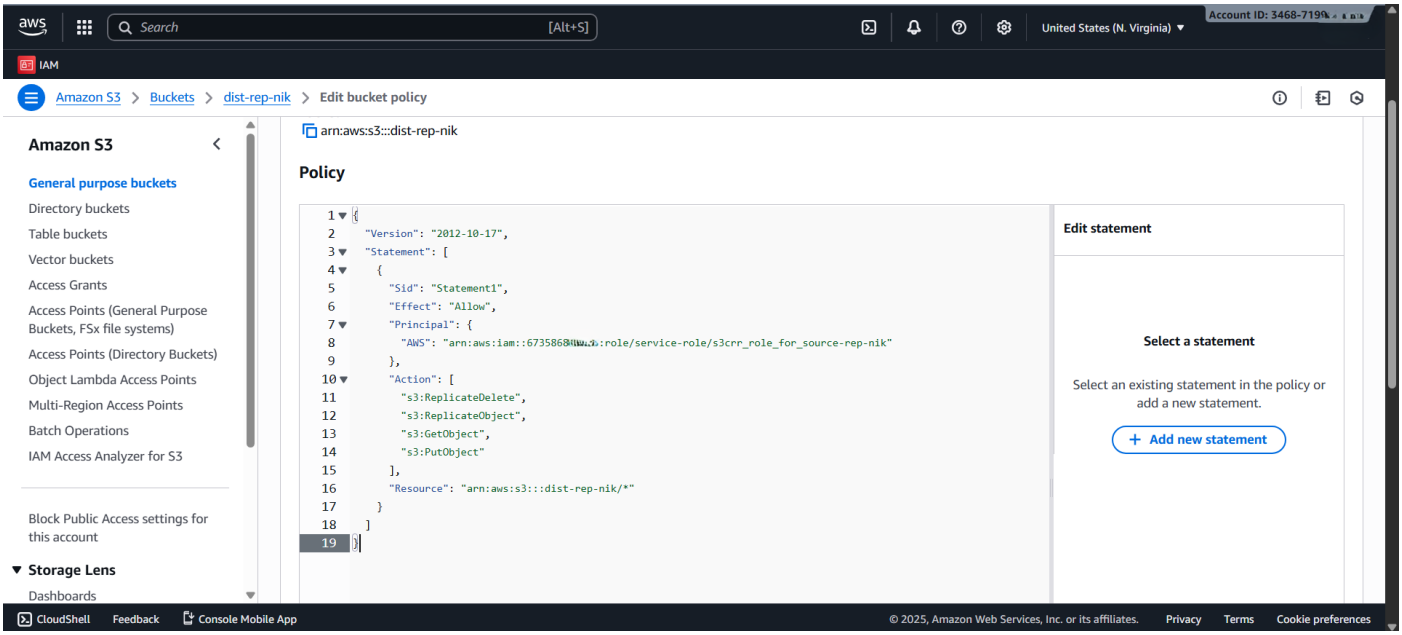




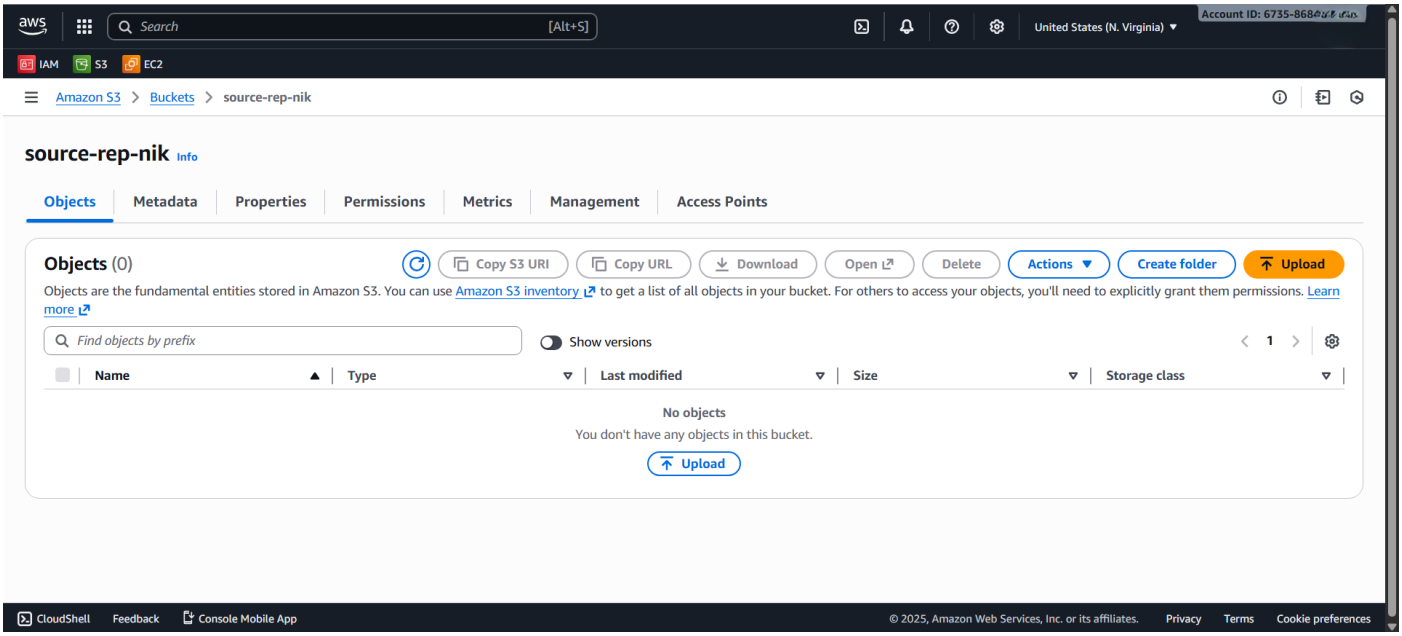
13. Copy this JSON and go back to Account B's S3 console, open the dist-rep-nik bucket Permissions tab, and edit the Bucket policy.

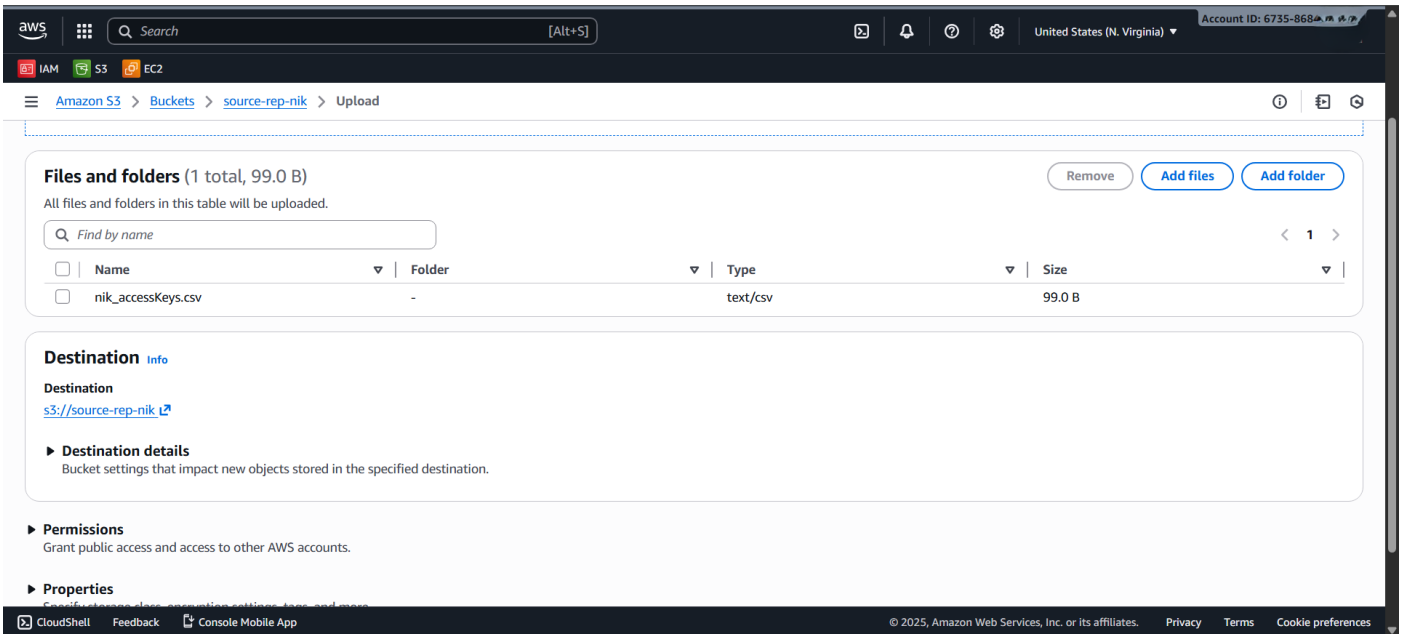


14. Paste the generated policy and save; the editor now shows the full bucket policy granting the replication role permissions on the destination bucket.

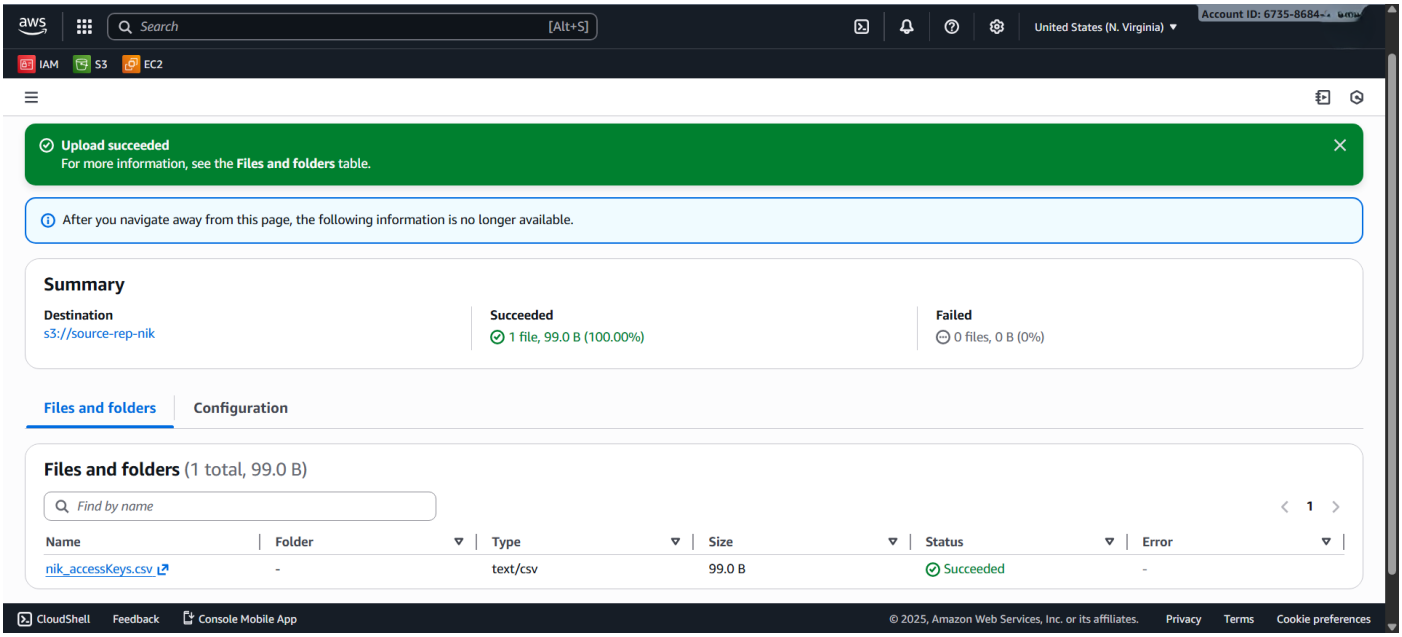


15. In the source-rep-nik bucket's Objects tab, click Upload, add a test file such as nik_accessKeys.csv, and start the upload.





16. The upload page shows the file listed under Files and folders with the destination s3://source-rep-nik, and once the upload completes the object appears in the source bucket.



17. After a short delay, open the dist-rep-nik bucket in Account B and confirm that the same object now appears there, proving that cross-account replication from Account A to Account B is working.