Q1. To pick a publicly available cloud migration industry example and to review their features and to use it as case study. Also to review the story and conduct a cloud journey analysis for the topics as mentioned.

Company Name: DiscoverX- AWS Cloud Migration Story.

DiscoverX Corporation:

DiscoverX founded in the year 2000, is dedicated to commercialization and development in drug research. It develops, manufactures a suite of products and services for pharma and biotech companies, allowing customers to get results in an efficient manner. Thereby improving safety and efficacy of drugs for the ones in the market.

Challenges Faced by the company:

- In order to deliver their services, the company had implemented a client-server architecture for a very long period of time. In order to use the services, the clients had to use a thin client application that connected with the application and database servers, managed by the employees of the company which were hosted on DiscoverX datacenter's.
- On addition of clients to the company database, to either scaling up the resources or to scale-down(for cost effectiveness) was a hiccup that the employees faced. Having a backup of data and resiliency was an additional challenge for them.

Goals behind cloud migration:

Business Drivers:

- The company wanted to optimize their operations from the traditional client-server model infrastructure on understanding the benefits cloud infrastructure can provide to their business needs.
- It further helped them reduce the management costs, by leveraging the cloud services of Amazon Web Services(AWS).
- Scalability was an added advantage for them on taking their datacentres to the cloud infrastructure.

Technology Drivers/Goals:

- Reducing Outage and having a backup for the data centre.
- They envisioned for a cloud based Software as a service model, which will eliminate their technical support overhead which included giving support with the desktop-based thin client.
- Reducing dependency on technical support, improving availability and ease of scalability can help them concentrate on their business and client needs.

Migration strategy used for cloud migration:

- DiscoverX partnered with a cloud solution provider, clearScale to design and implement their SaaS platform on AWS. New cusomers directly boarded to SaaS platform and existing custmers had to be migrated to the platform.
- Services of AWS implemented for the organisation include: Elastic Load Balancers(ELB), CloudTail, CloudWatch, Identity Access Management(IAM), Virtual Private Networks(VPCs), and Availability Zones (AZs), EC2 Container Registry.

- Elastic Beanstalk service managed the deployment of application infrastructure components, which included ELBs, ECS, docker and clusters.

Organizational Change:

- Development and Production Cloud was stripped across two AZs for both redundancy and availability of the SaaS application.
- From the initial Client server architecture, after moving to cloud each AZ was configured with two subnets, Public and Private subnet. Public subnet hosting the Elastic Load Balancers, NAT gateways and bastion hosts.
- While, private subnet hosts the EC2 container services running Java and AngularJS containers.

Migration Journey:

- They are Building all mission-critical components on AWS services, taking use of all the benefits of world-class infrastructure/services while offloading IT burden associated with infrastructure management, while completing most of the critical services to the cloud they are still in the journey to take their infrastructure completely cloud based.
- DiscoverX uses CloudFormation to create and manage virtual network infrastructure as well as Postgres RDS instances. This sets the groundwork for the application layer and may be reused to construct further VPCs or deployments in different AWS Regions.

Where are they now in the Journey?

- After moving most of the services while still having a need to access their legacy systems, they have developed an Oracle to Postgres data pipeline in order to keep the already developed oracle database and Postgres RDS in synchronization.
- This is a crucial component in ensuring a seamless transition of clients from traditional to SaaS.

Lessons Learnt:

- Elastic Beanstalk can be used to manage application infrastructure as it integrates well with ECS, container deployments for auto-scaling and ELBs.
- Using Elastic Beanstalks is a simple-to-use solution with proven dependability that works well with blue/green deployment techniques.
- Technique of ECS cluster management can be used, while docker containers may be created and deployed for an effective deployment strategy. ELBs can be created, managed and be setup for auto-scaling.

Outcomes Achieved:

- DiscoverX now has a solid Software as a Service (SaaS) delivery model. They reap the benefits of availability and redundancy from the AWS platform.
- Auto scaling capabilities achieved from cloud provider offered cost savings and enabled unparallel growth.

- They are able to shorten the time it takes to offer new analytical solutions and features to their clients.
- The faster development cycle is thus helping them raise the degree of innovation and thereby helps them distinguish the brand.

My recommended Cloud Migration Strategy if to be embarked on the journey of cloud deployment:

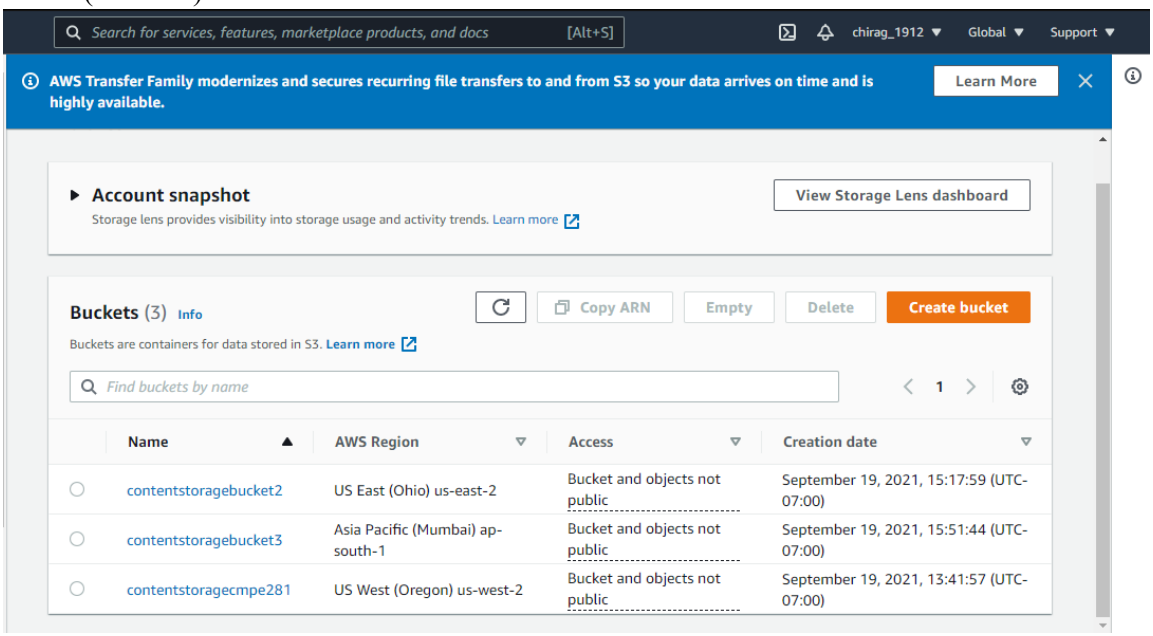
- Production VPC can be divided to more than two different Availability Zones for the extended/ added availability and redundancy of the services.
- While the AZs can be configured with subnets of Public and private ones. With Public subnet hosting the ELBs, and used for hosting. While private one used for container services.
- A Postgres RDS multi-AZ deployment with the Master setup in the first AZ and a Standby and Read Replica in the second availability zone.
- Implement auto scaling to provide elasticity of the application containers and the infrastructure using ECS based on the utilization.
- All the services can be load balanced for higher availability across the Availability Zones. While staging and production can be deployed on different instances to provide isolation, security and implement IAM rules for control of the services.
- Thereby, building these services can help the company leverage benefits of the infrastructure provided by AWS and will help offload the backlogs/overheads on their traditional infrastructure management.

CMPE 281 Cloud Storage Question #2:

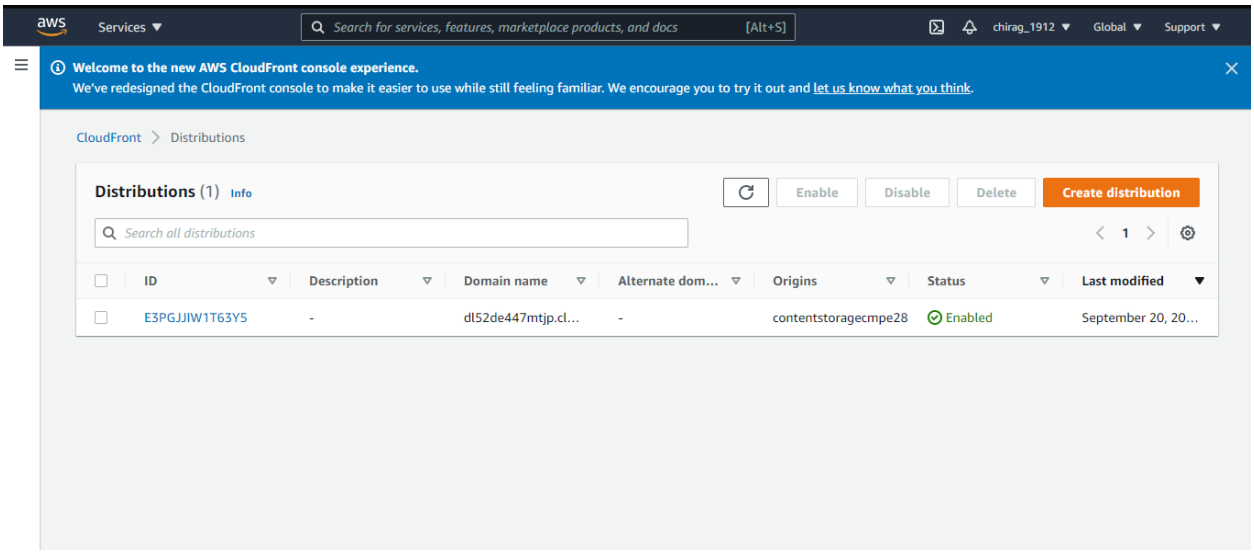
To implement delivery infrastructure on AWS to meet the requirements stated:

Availability and Low Latency:

1. We create buckets in different geographic regions to achieve availability.
   Also, by creating CDN (CloudFront) we create the cache to reduce the latency.
   S3 buckets created for availability in the region: US-East(Oregon), US West(Ohio) and Asia Pacific(Mumbai).

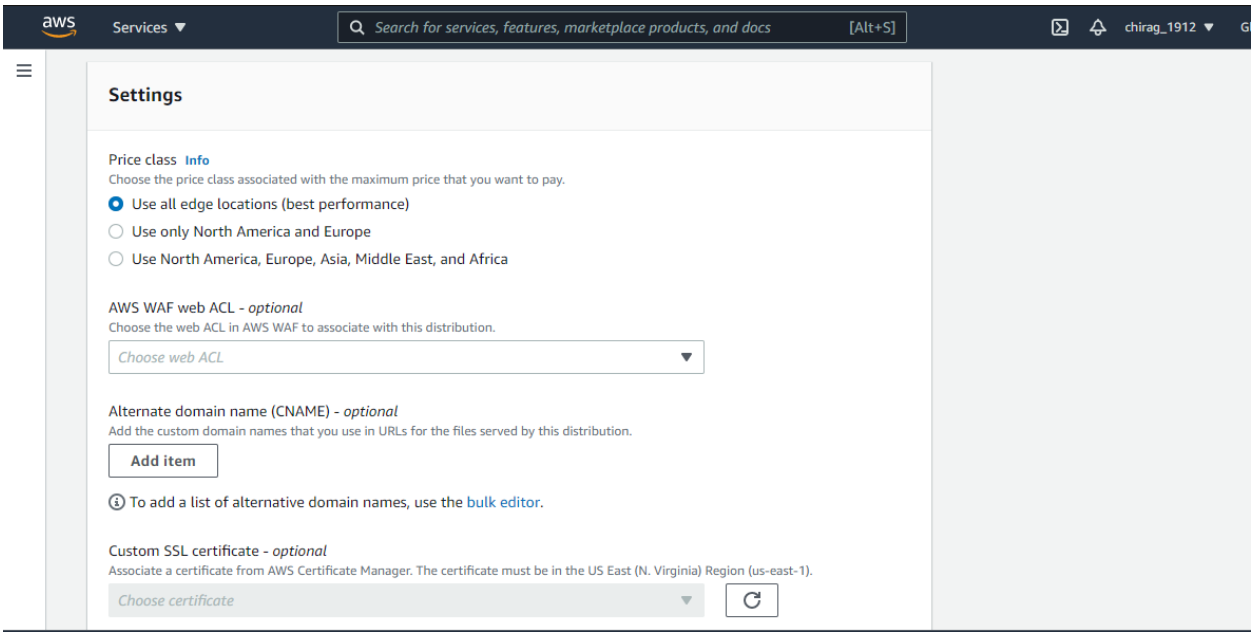


1a. To achieve low latency CDN (cloud-front) is used. Screenshot for creation of cloud front:



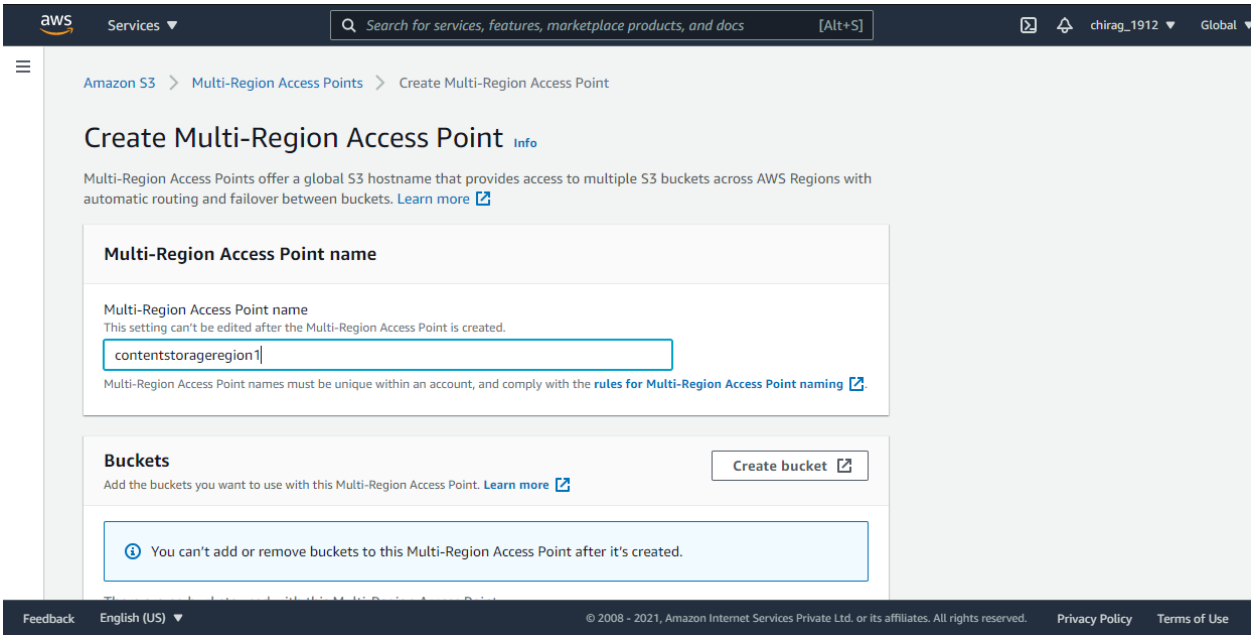
Properties of the cloud-front include:

a. Using all edge locations for the best performance (cache creation)
b. Using HTTP/2 version protocol and,
c. Using IPv6 address to cover multiple users in the cloud infrastructure.



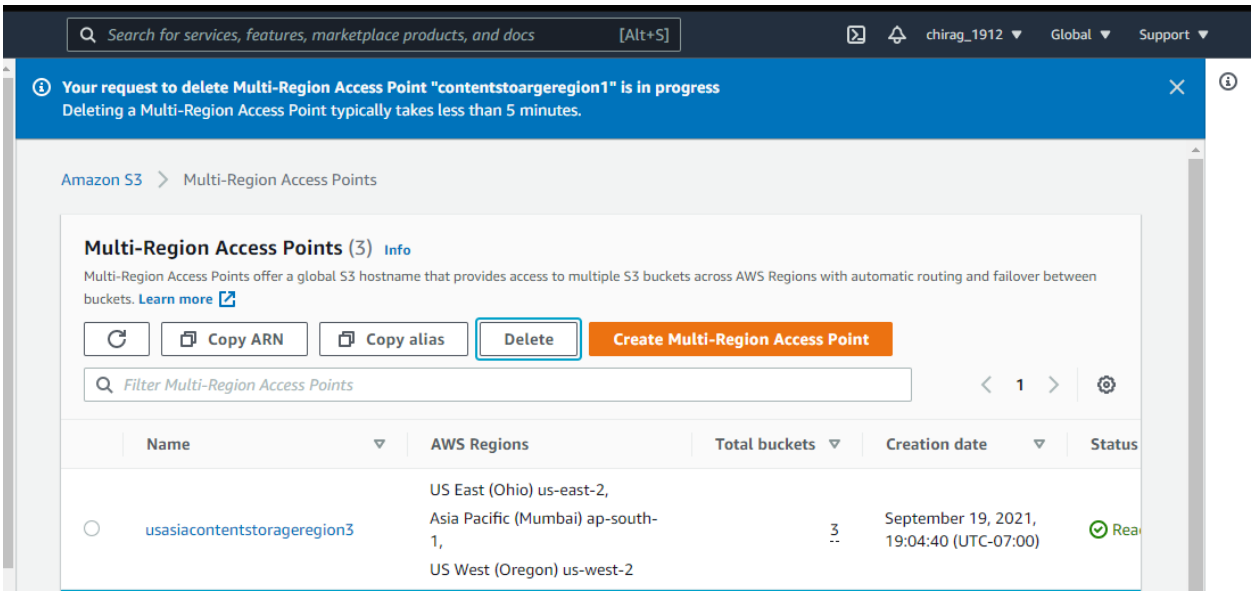
2. To reduce load on the origin multi-region access point is created:

1. Creating Multi region access points reduces the load on origin server and ensures availability.

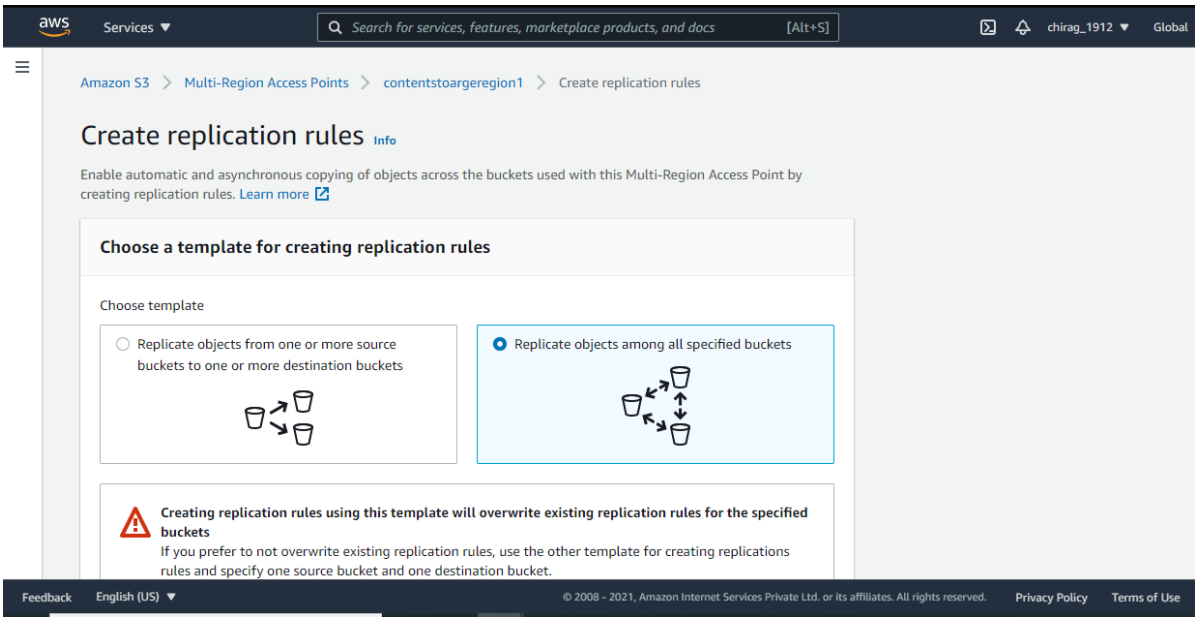


2. Multiple-Region Access Point created for US-East server. Thereby traffic will be redirected toward the nearest AWS region or the one with lowest latency issues, reducing unnecessary traffic back to S3 origin to help improve latency and reducing load on the origin.

Also, the replication of data to multiple S3 buckets will help in disaster recovery.

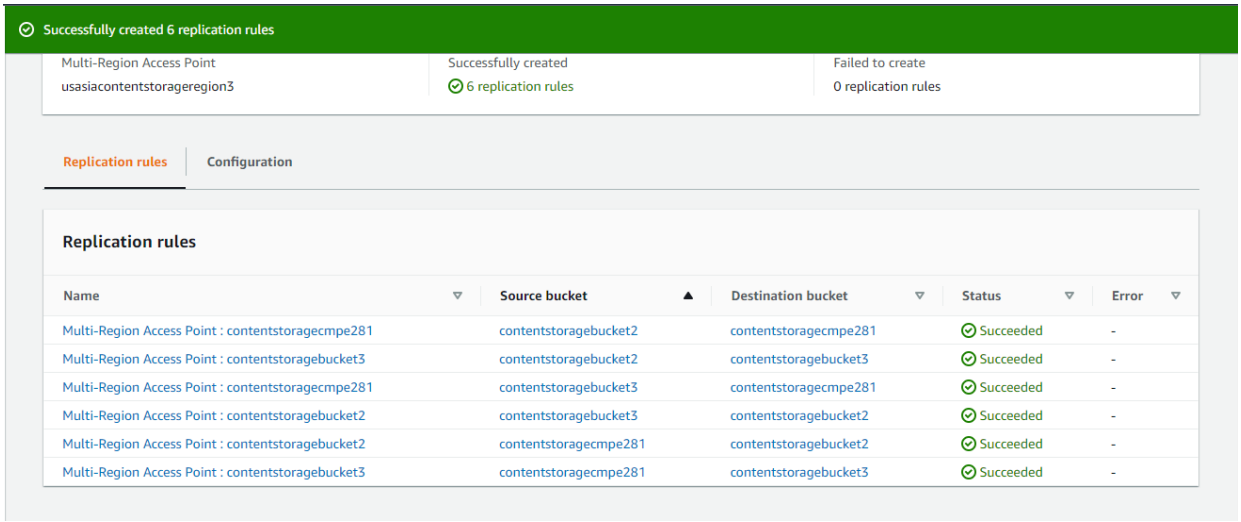


3. Replication rules can be set for the S3 buckets created and included in multi region setup.

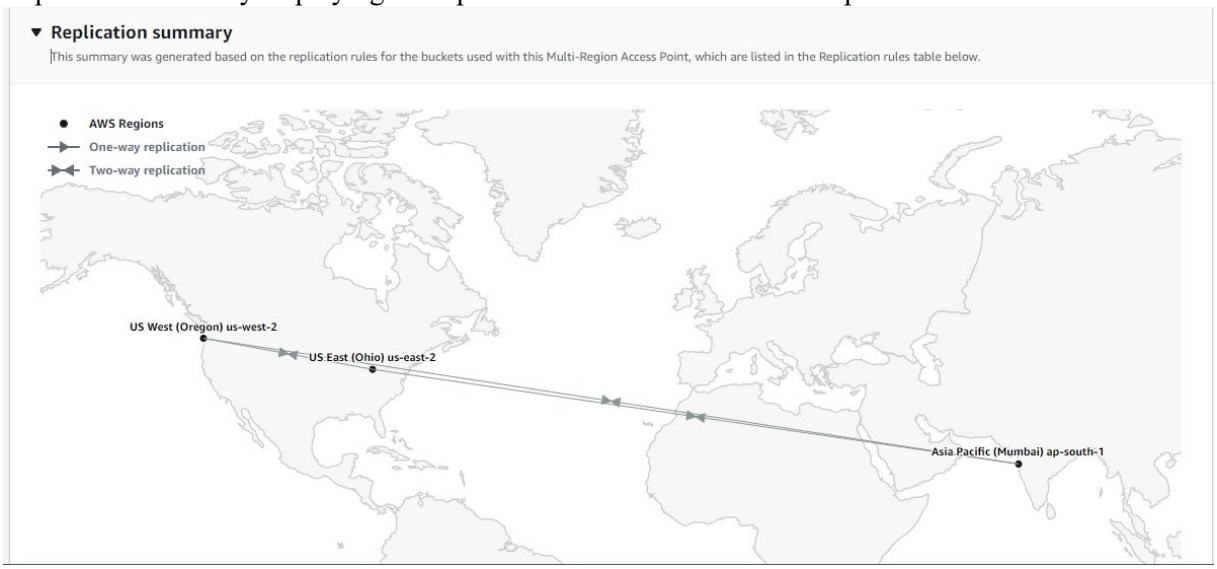


4. Replication rules created for the different regions of the S3 bucket:

Contentstoragecmpe281, contentstoragebucket2 and contentstoragebucket3

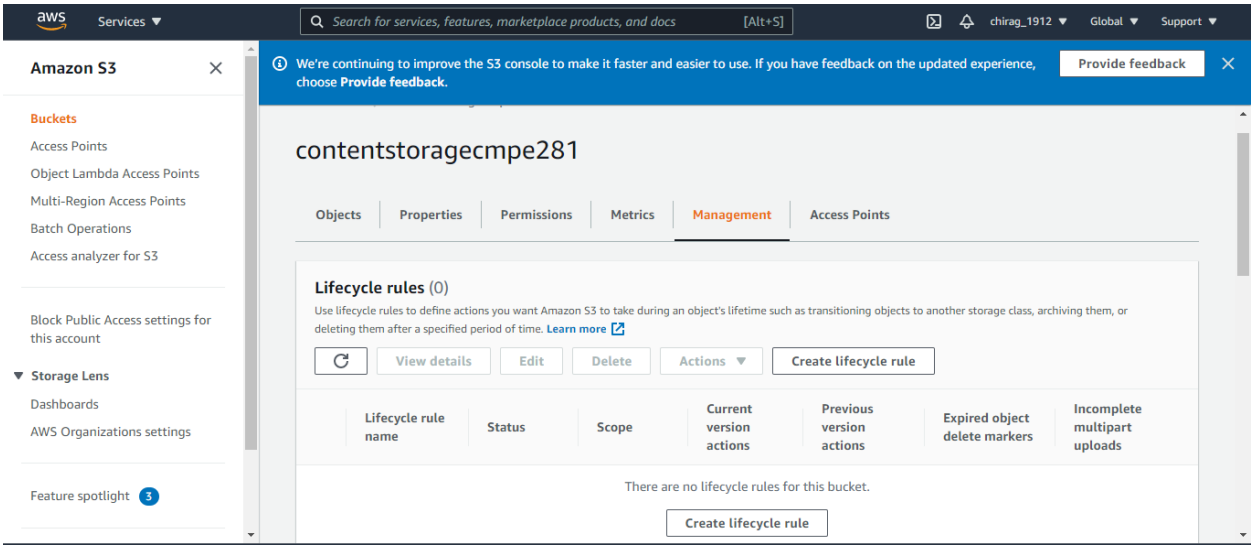


Replication summary displaying the replication of the data for the multiple buckets.

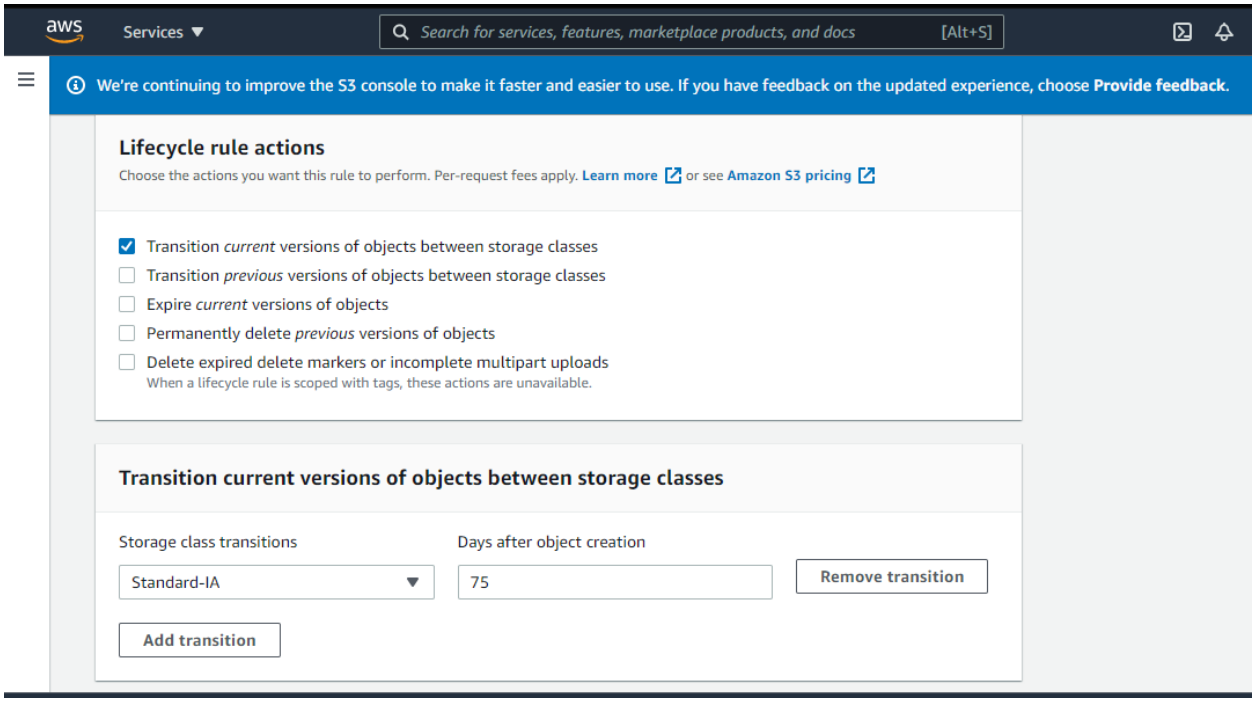


3. Life Cycle rules for the S3 Bucket:

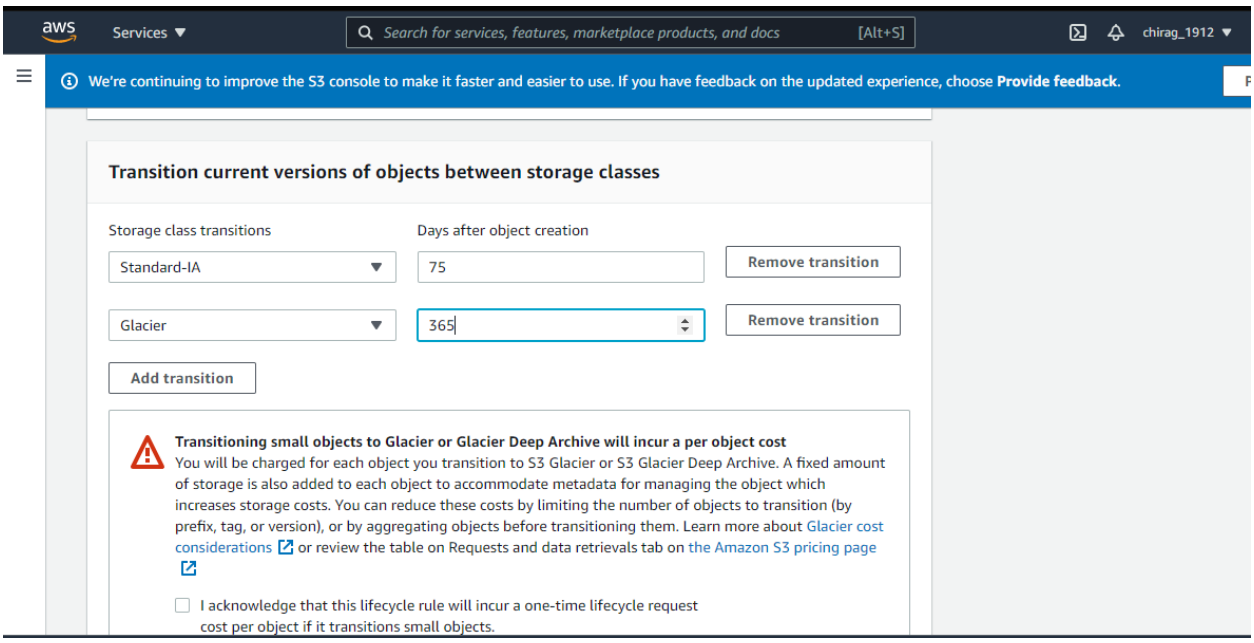
1. To create lifecycle rule for first bucket ensuring that data moves from active S3 bucket to different storage services based on usage pattern of the client.



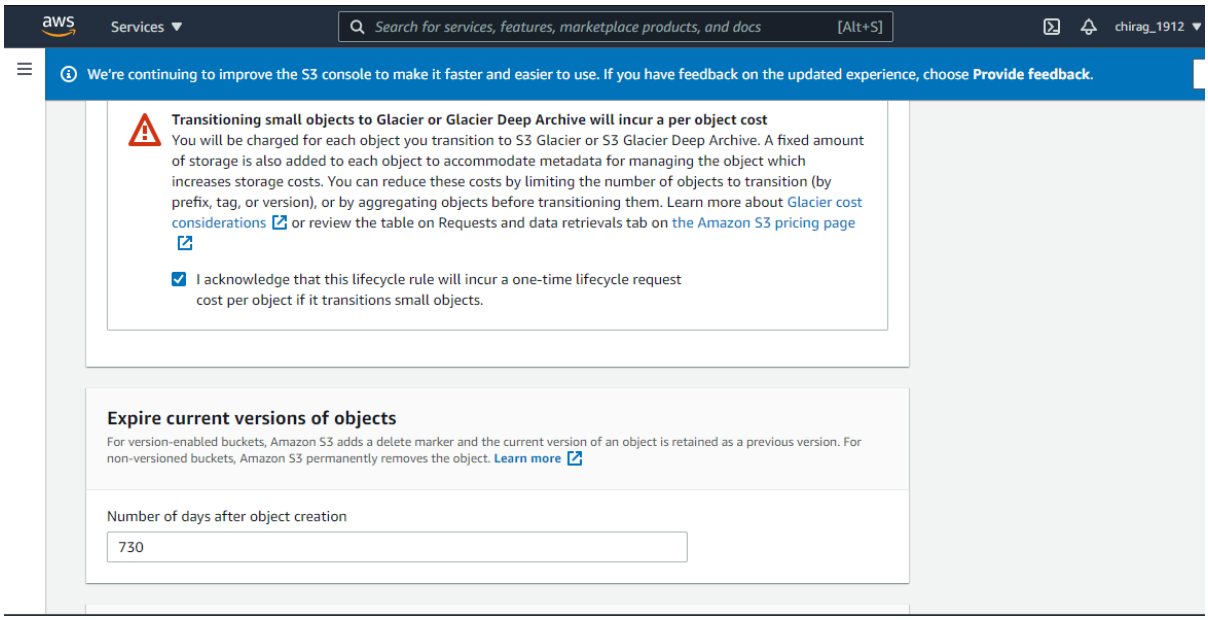
2. Using standard IA after 75 days of active usage(For infrequent access data, min storage duration of 30 days).



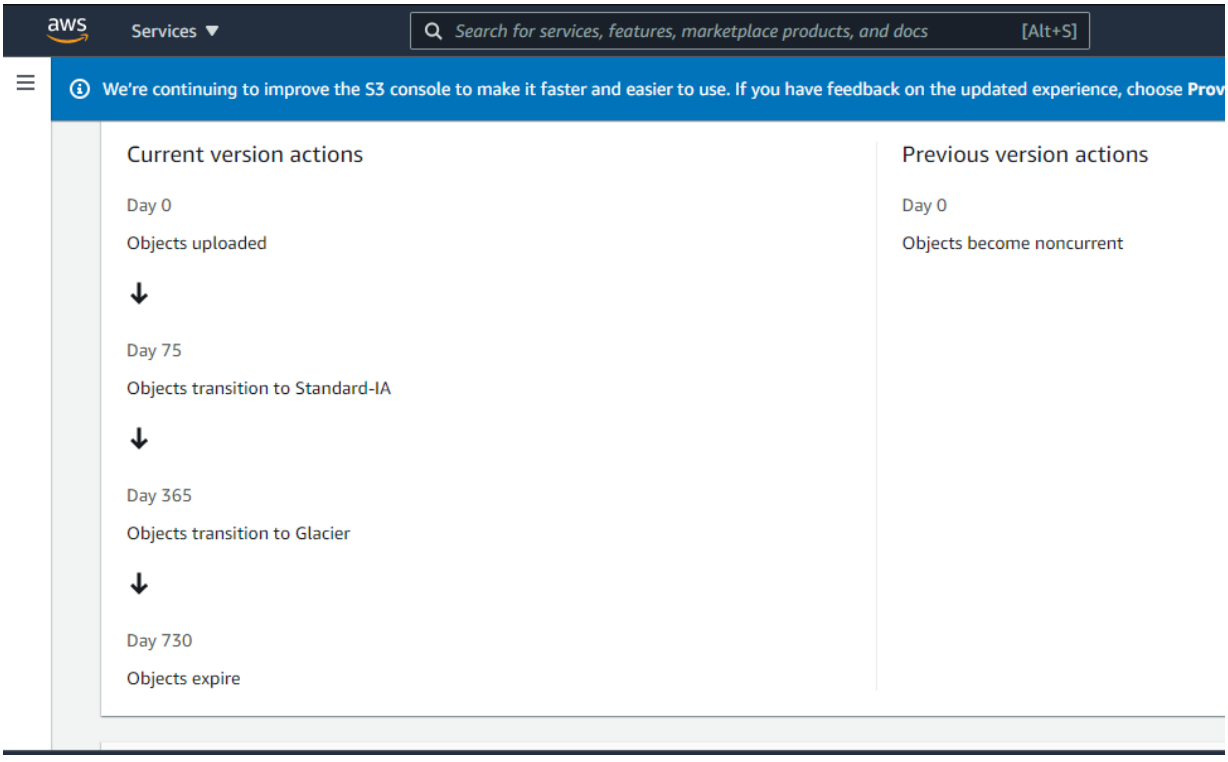
3. Using S3 Glacier after 365 days of infrequent access in IA storage.



4. Setting objects to expire after 730 days of S3 object creation date.

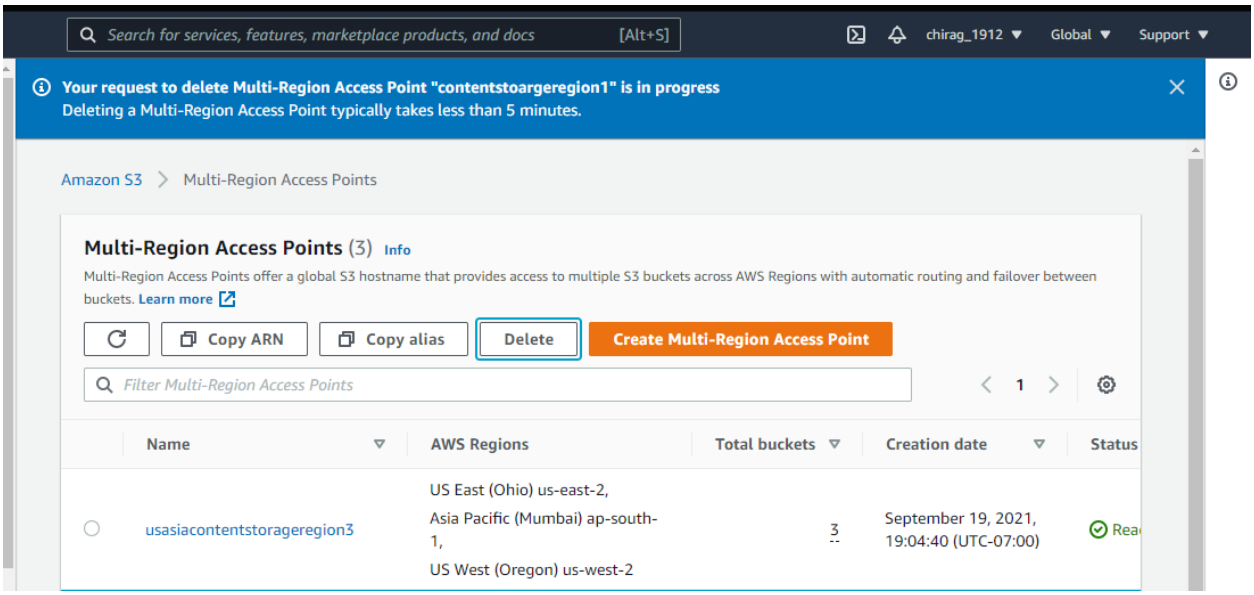


5. Summary of the lifecycle management for the object instance created.

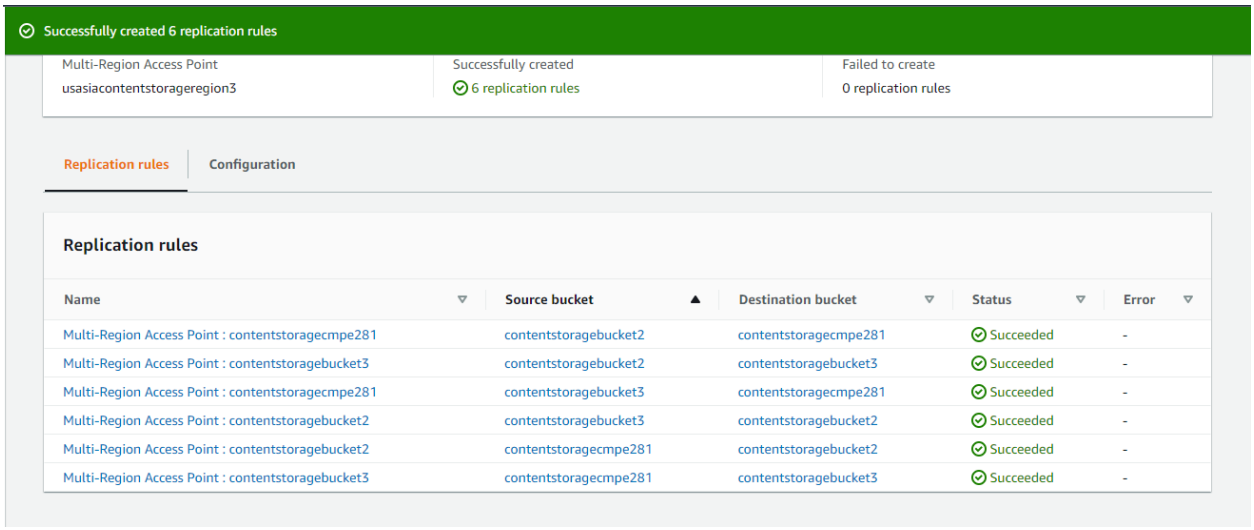


4. Disaster Recovery(DR) to be implemented:

1. To have disater recover for the AWS setup, the multiregion access point with replication created for multiple AWS regions, can serve the purpose.



2. Rules set for disaster recovery. Creating copies of data backup for eah of the buckets created.

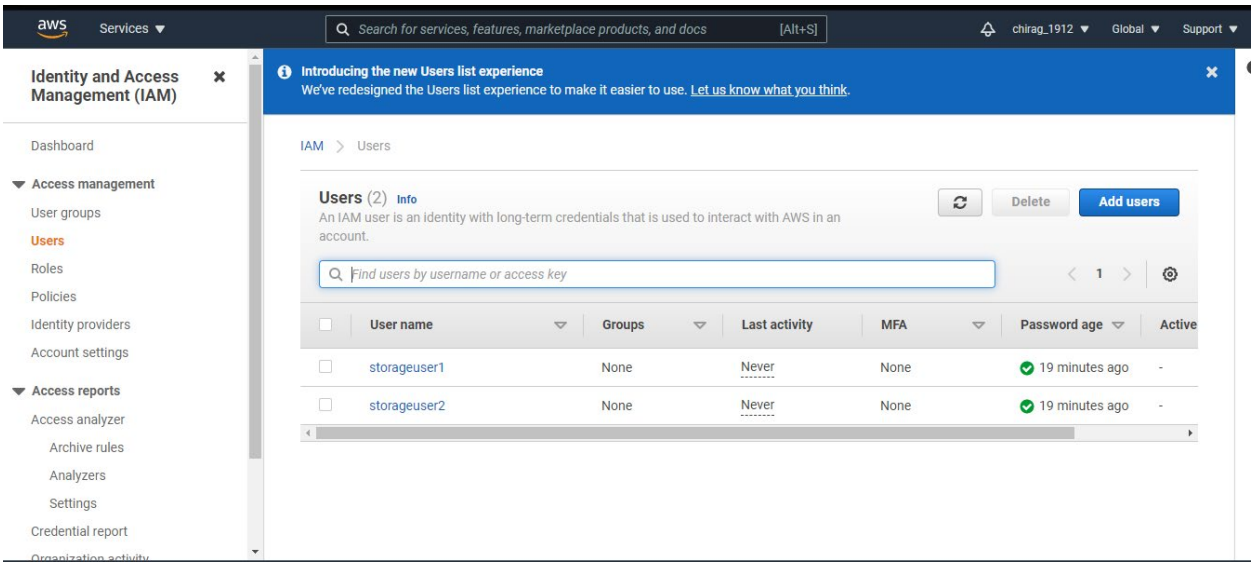


3. Summary for the Disaster recovery(replicas created) showing the transfer/backup of data between multiple regions:

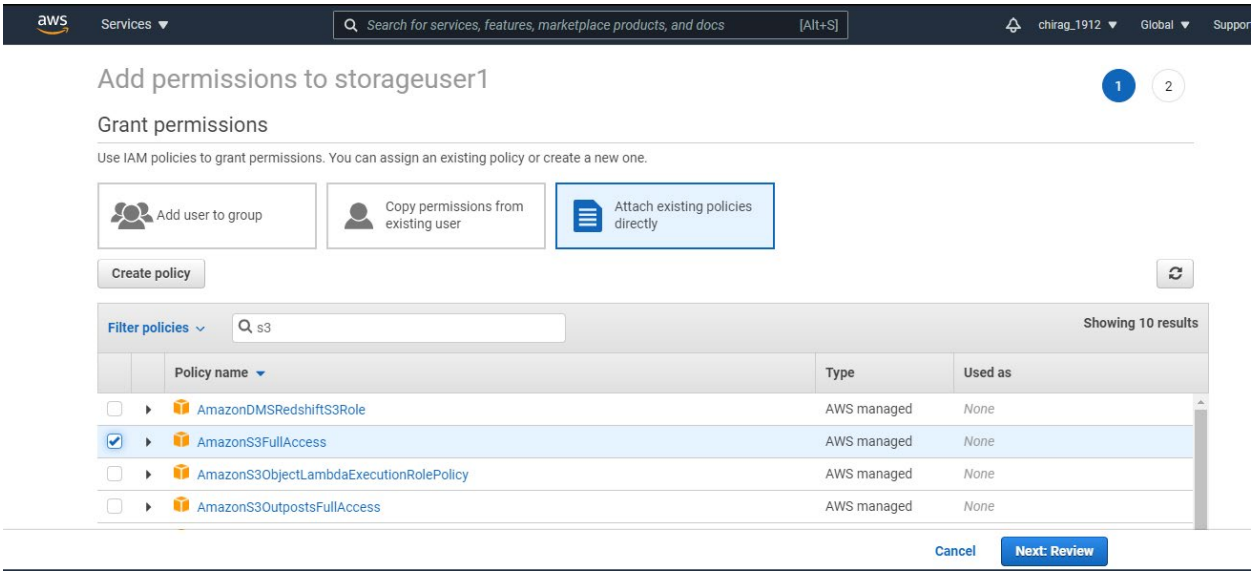
5. Acess to authorized users only:

Creating Identity Access Management permissions: Two application users are created:

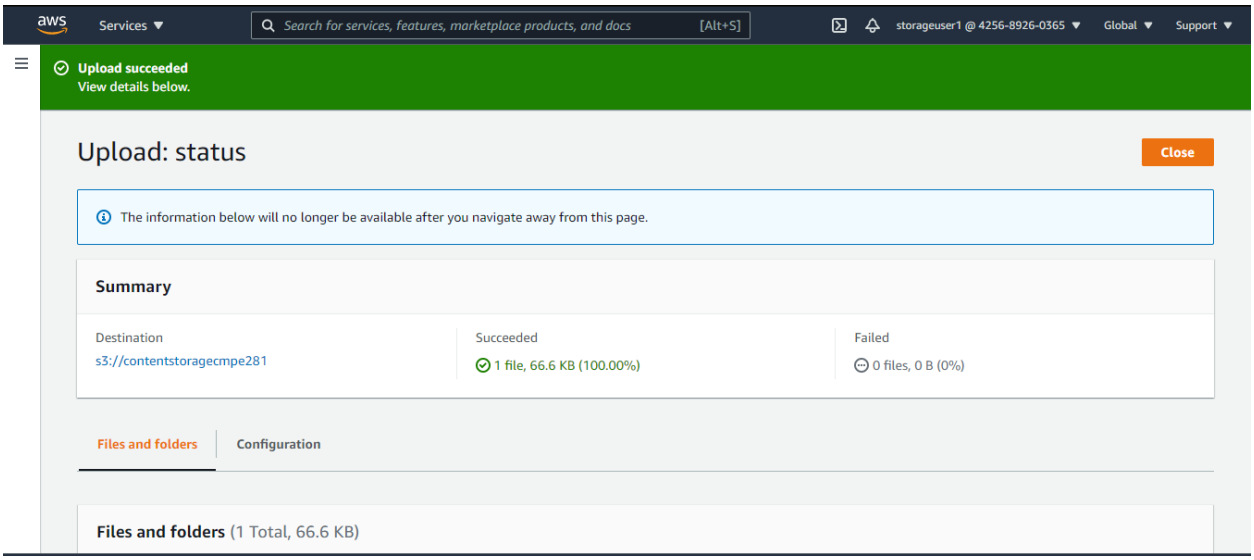
1. Storage user1(with read/write permission),
2. Storage user2(with no permission to either read write) date to the AWS instances.



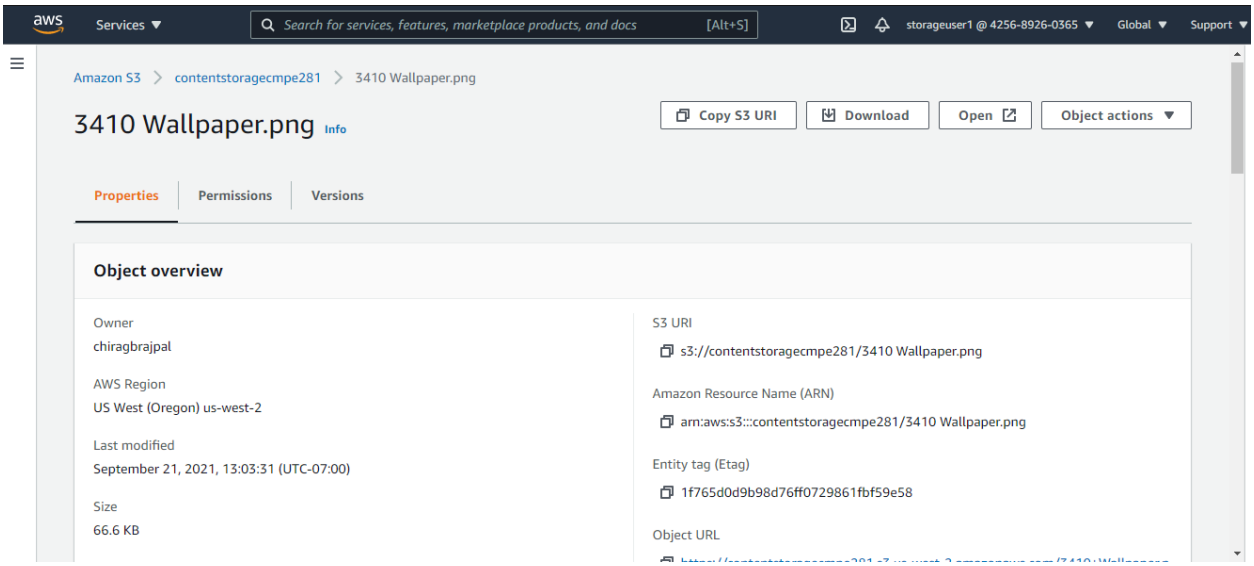
3. Storage User 1 given permission S3 Full Access(including read/write). Which enables the user to upload and downlaod the files from the S3 bucket for which the permission is granted.



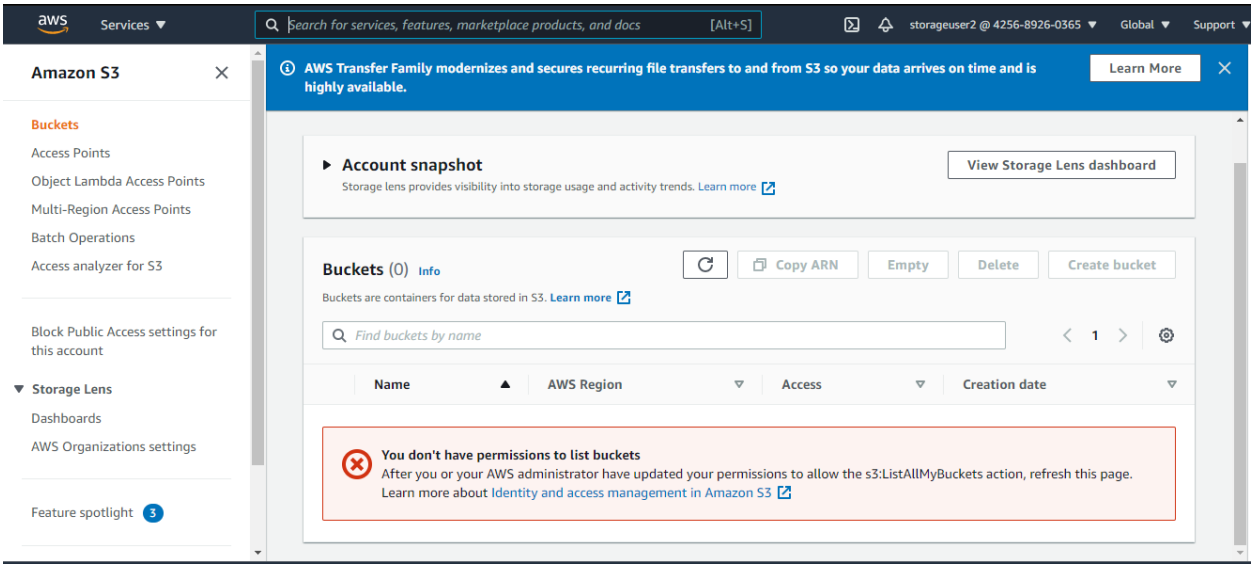
4. Logging in with User1 to showcase user1 has full access for downlaod/upload operations: File has been uploaded by the user1 to S3 bucket (storagecontainercmpe281).



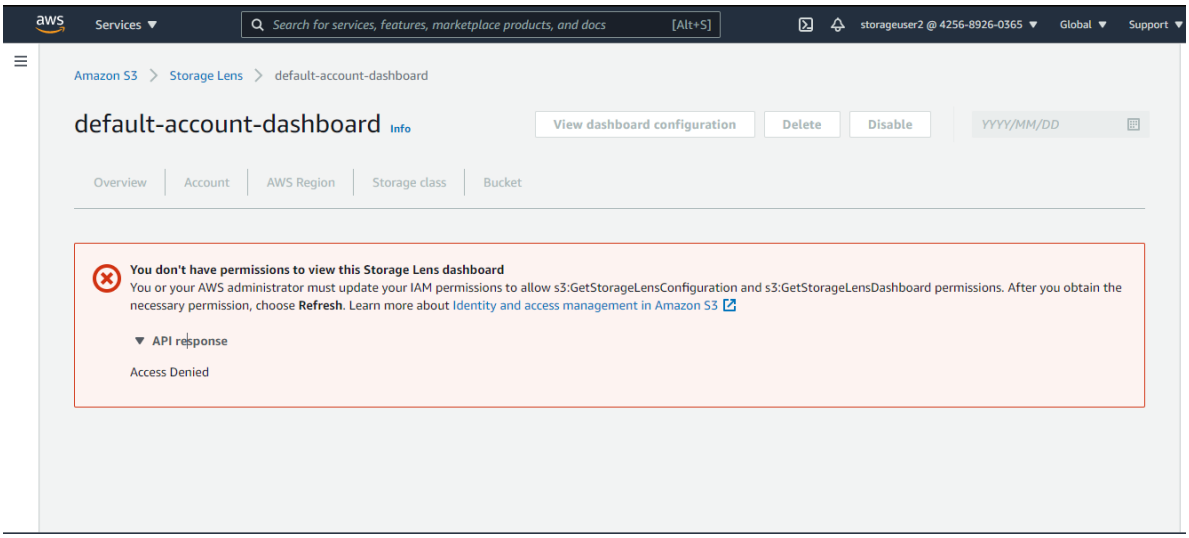
5. Option for file download is visible and accessible to the first storage user1.



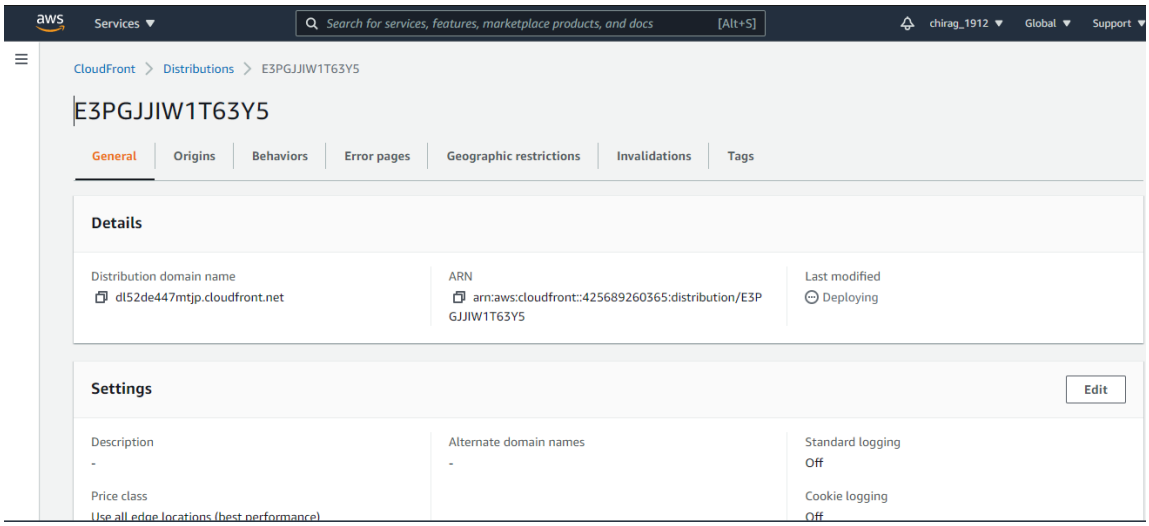
6. For storageuser2 permissions for download and upload is not provided:



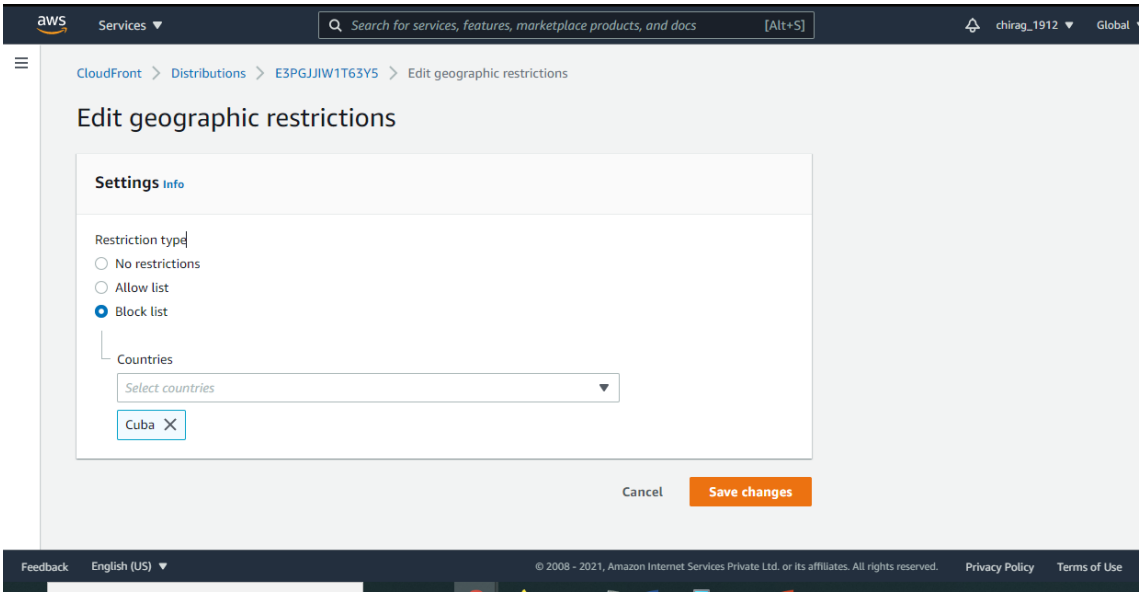
7. Permissions denied for the storageuser2 which is not given read/write permission in IAM:



6. **To block access of IP connections coming from a particular region**:
    1. Distribution(E3PGJJIW1T63Y5) created in Cloud Front in order to block access.



2. Adding Blocklist for Cuba Teritorry in block region tab of the CloudFront.
   The cloud front takes care of blocking the ping/ip requests coming from the Cuba region.



Architecture Diagram: