

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 customers directly boarded to SaaS platform and existing customers had to be migrated to the platform.
- Services of AWS implemented for the organisation include: Elastic Load Balancers(ELB), CloudTrail, 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:

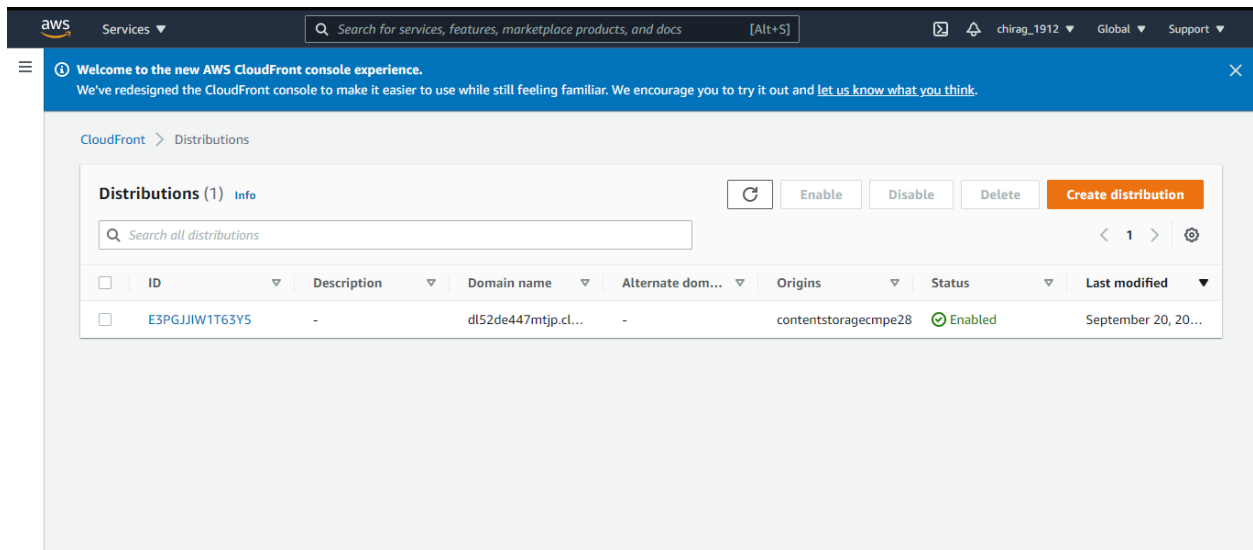
Availability and Low Latency:

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).

The screenshot shows the AWS Management Console interface for the S3 service. At the top, there is a search bar and navigation links. Below the navigation bar, a blue banner advertises the AWS Transfer Family. The main content area is titled 'Buckets (3)' and includes a 'View Storage Lens dashboard' button. Below this, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. A search bar for finding buckets by name is present. The main table lists the following buckets:

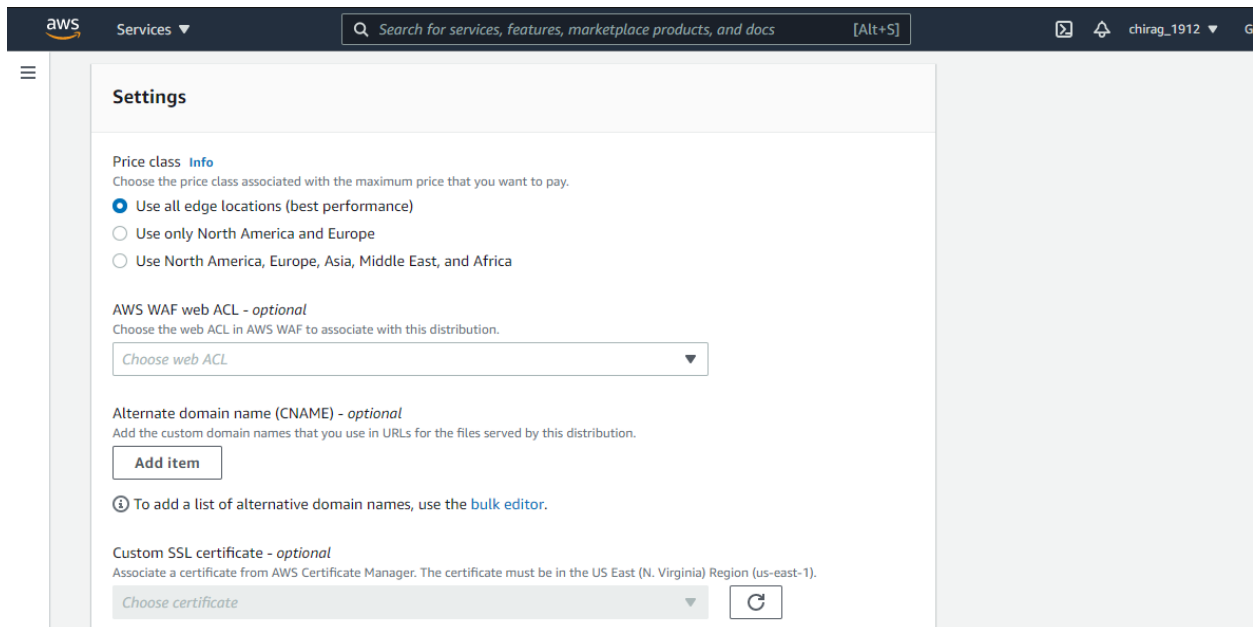
	Name	AWS Region	Access	Creation date
<input type="radio"/>	contentstoragebucket2	US East (Ohio) us-east-2	Bucket and objects not public	September 19, 2021, 15:17:59 (UTC-07:00)
<input type="radio"/>	contentstoragebucket3	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	September 19, 2021, 15:51:44 (UTC-07:00)
<input type="radio"/>	contentstoragecmpe281	US West (Oregon) us-west-2	Bucket and objects not public	September 19, 2021, 13:41:57 (UTC-07:00)

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



Properties of the cloud-front include:

- Using all edge locations for the best performance (cache creation)
- Using HTTP/2 version protocol and,
- 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.

The screenshot shows the 'Create Multi-Region Access Point' page in the AWS console. The breadcrumb navigation is 'Amazon S3 > Multi-Region Access Points > Create Multi-Region Access Point'. The main heading is 'Create Multi-Region Access Point' with an 'Info' link. Below the heading, a description states: 'Multi-Region Access Points offer a global S3 hostname that provides access to multiple S3 buckets across AWS Regions with automatic routing and failover between buckets. [Learn more](#)'. The 'Multi-Region Access Point name' section contains a text input field with 'contentstorageregion1'. A note below the field says: 'Multi-Region Access Point names must be unique within an account, and comply with the [rules for Multi-Region Access Point naming](#)'. The 'Buckets' section has a 'Create bucket' button and a message: 'You can't add or remove buckets to this Multi-Region Access Point after it's created.'

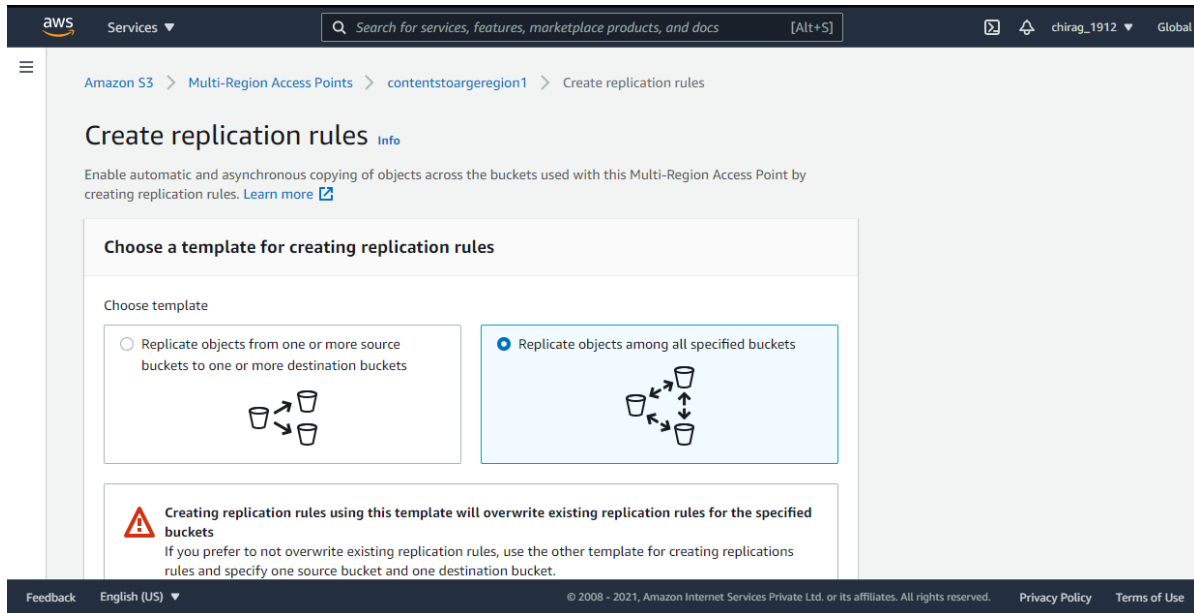
2. Multiple-Region Access Point created for US-East server. Thereby traffic will be redirected toward the nearest AWS region or the one with lowest latency issues, reducing unnecessary traffic back to S3 origin to help improve latency and reducing load on the origin.

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

The screenshot shows the 'Multi-Region Access Points' list page in the AWS console. A blue banner at the top states: 'Your request to delete Multi-Region Access Point "contentstoargeregion1" is in progress. Deleting a Multi-Region Access Point typically takes less than 5 minutes.' Below the banner, the page title is 'Multi-Region Access Points (3)' with an 'Info' link. A description states: 'Multi-Region Access Points offer a global S3 hostname that provides access to multiple S3 buckets across AWS Regions with automatic routing and failover between buckets. [Learn more](#)'. Action buttons include 'Refresh', 'Copy ARN', 'Copy alias', 'Delete', and 'Create Multi-Region Access Point'. A search bar is labeled 'Filter Multi-Region Access Points'. The table below lists the access points.

	Name	AWS Regions	Total buckets	Creation date	Status
<input type="radio"/>	usasiacontentstorageregion3	US East (Ohio) us-east-2, Asia Pacific (Mumbai) ap-south-1, US West (Oregon) us-west-2	3	September 19, 2021, 19:04:40 (UTC-07:00)	Ready

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



- Replication rules created for the different regions of the S3 bucket:

Contentstoragecmpe281, contentstoragebucket2 and contentstoragebucket3

Successfully created 6 replication rules

Multi-Region Access Point
usasiaccontentstorageregion3

Successfully created
6 replication rules

Failed to create
0 replication rules

Replication rules

Configuration

Replication rules

Name	Source bucket	Destination bucket	Status	Error
Multi-Region Access Point : contentstoragecmpe281	contentstoragebucket2	contentstoragecmpe281	✔ Succeeded	-
Multi-Region Access Point : contentstoragebucket3	contentstoragebucket2	contentstoragebucket3	✔ Succeeded	-
Multi-Region Access Point : contentstoragecmpe281	contentstoragebucket3	contentstoragecmpe281	✔ Succeeded	-
Multi-Region Access Point : contentstoragebucket2	contentstoragebucket3	contentstoragebucket2	✔ Succeeded	-
Multi-Region Access Point : contentstoragebucket2	contentstoragecmpe281	contentstoragebucket2	✔ Succeeded	-
Multi-Region Access Point : contentstoragebucket3	contentstoragecmpe281	contentstoragebucket3	✔ Succeeded	-

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.

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

chirag_1912 Global Support

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

contentstoragecmpe281

Objects Properties Permissions Metrics **Management** Access Points

Lifecycle rules (0)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

View details Edit Delete Actions Create lifecycle rule

Lifecycle rule name	Status	Scope	Current version actions	Previous version actions	Expired object delete markers	Incomplete multipart uploads
There are no lifecycle rules for this bucket.						

Create lifecycle rule

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

Lifecycle rule actions
Choose the actions you want this rule to perform. Per-request fees apply. [Learn more](#) or see [Amazon S3 pricing](#)

- ☒ Transition *current* versions of objects between storage classes
- ☐ Transition *previous* versions of objects between storage classes
- ☐ Expire *current* versions of objects
- ☐ Permanently delete *previous* versions of objects
- ☐ Delete expired delete markers or incomplete multipart uploads

When a lifecycle rule is scoped with tags, these actions are unavailable.

Transition current versions of objects between storage classes

Storage class transitions: Standard-IA (dropdown)
Days after object creation: 75 (input field)
[Remove transition](#)
[Add transition](#)

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

Transition current versions of objects between storage classes

Storage class transitions: Standard-IA (dropdown)
Days after object creation: 75 (input field)
[Remove transition](#)

Storage class transitions: Glacier (dropdown)
Days after object creation: 365 (input field)
[Remove transition](#)
[Add transition](#)

⚠️ Transitioning small objects to Glacier or Glacier Deep Archive will incur a per object cost
You will be charged for each object you transition to S3 Glacier or S3 Glacier Deep Archive. A fixed amount of storage is also added to each object to accommodate metadata for managing the object which increases storage costs. You can reduce these costs by limiting the number of objects to transition (by prefix, tag, or version), or by aggregating objects before transitioning them. [Learn more about Glacier cost considerations](#) or review the table on Requests and data retrievals tab on the [Amazon S3 pricing page](#)

☐ I acknowledge that this lifecycle rule will incur a one-time lifecycle request cost per object if it transitions small objects.

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

aws Services [Alt+S] chirag_1912

ⓘ We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose **Provide feedback**.

⚠ Transitioning small objects to Glacier or Glacier Deep Archive will incur a per object cost
You will be charged for each object you transition to S3 Glacier or S3 Glacier Deep Archive. A fixed amount of storage is also added to each object to accommodate metadata for managing the object which increases storage costs. You can reduce these costs by limiting the number of objects to transition (by prefix, tag, or version), or by aggregating objects before transitioning them. [Learn more about Glacier cost considerations](#) or review the table on Requests and data retrievals tab on the [Amazon S3 pricing page](#)

☒ I acknowledge that this lifecycle rule will incur a one-time lifecycle request cost per object if it transitions small objects.

Expire current versions of objects
For version-enabled buckets, Amazon S3 adds a delete marker and the current version of an object is retained as a previous version. For non-versioned buckets, Amazon S3 permanently removes the object. [Learn more](#)

Number of days after object creation

730

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

aws Services <input type="text" value="Search for services, features, marketplace products, and docs"/> [Alt+S]	
ⓘ We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback .	
Current version actions	Previous version actions
Day 0	Day 0
Objects uploaded	Objects become noncurrent
↓	
Day 75	
Objects transition to Standard-IA	
↓	
Day 365	
Objects transition to Glacier	
↓	
Day 730	
Objects expire	

4. Disaster Recovery(DR) to be implemented:

1. To have disaster recovery for the AWS setup, the multi-region access point with replication created for multiple AWS regions, can serve the purpose.

Search for services, features, marketplace products, and docs

[Alt+S]

chirag_1912

Global

Support

Your request to delete Multi-Region Access Point "contentstoargeregion1" is in progress

Deleting a Multi-Region Access Point typically takes less than 5 minutes.

Amazon S3

Multi-Region Access Points

Multi-Region Access Points (3)

Info

Multi-Region Access Points offer a global S3 hostname that provides access to multiple S3 buckets across AWS Regions with automatic routing and failover between buckets. [Learn more](#)

Copy ARN

Copy alias

Delete

Create Multi-Region Access Point

Filter Multi-Region Access Points

< 1 >

Name	AWS Regions	Total buckets	Creation date	Status
<div><div></div>usasiacontentstorageregion3</div>	US East (Ohio) us-east-2, Asia Pacific (Mumbai) ap-south-1, US West (Oregon) us-west-2	3	September 19, 2021, 19:04:40 (UTC-07:00)	Ready

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

Successfully created 6 replication rules

Multi-Region Access Point
usasiacontentstorageregion3

Successfully created
6 replication rules

Failed to create
0 replication rules

Replication rules

Configuration

Replication rules

Name	Source bucket	Destination bucket	Status	Error
Multi-Region Access Point : contentstoragecmpe281	contentstoragebucket2	contentstoragecmpe281	Succeeded	-
Multi-Region Access Point : contentstoragebucket3	contentstoragebucket2	contentstoragebucket3	Succeeded	-
Multi-Region Access Point : contentstoragecmpe281	contentstoragebucket3	contentstoragecmpe281	Succeeded	-
Multi-Region Access Point : contentstoragebucket2	contentstoragebucket3	contentstoragebucket2	Succeeded	-
Multi-Region Access Point : contentstoragebucket2	contentstoragecmpe281	contentstoragebucket2	Succeeded	-
Multi-Region Access Point : contentstoragebucket3	contentstoragecmpe281	contentstoragebucket3	Succeeded	-

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



5. Access to authorized users only:

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

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

aws Services

Search for services, features, marketplace products, and docs [Alt+S]

chirag_1912 Global Support

Identity and Access Management (IAM)

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity

Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

IAM > Users

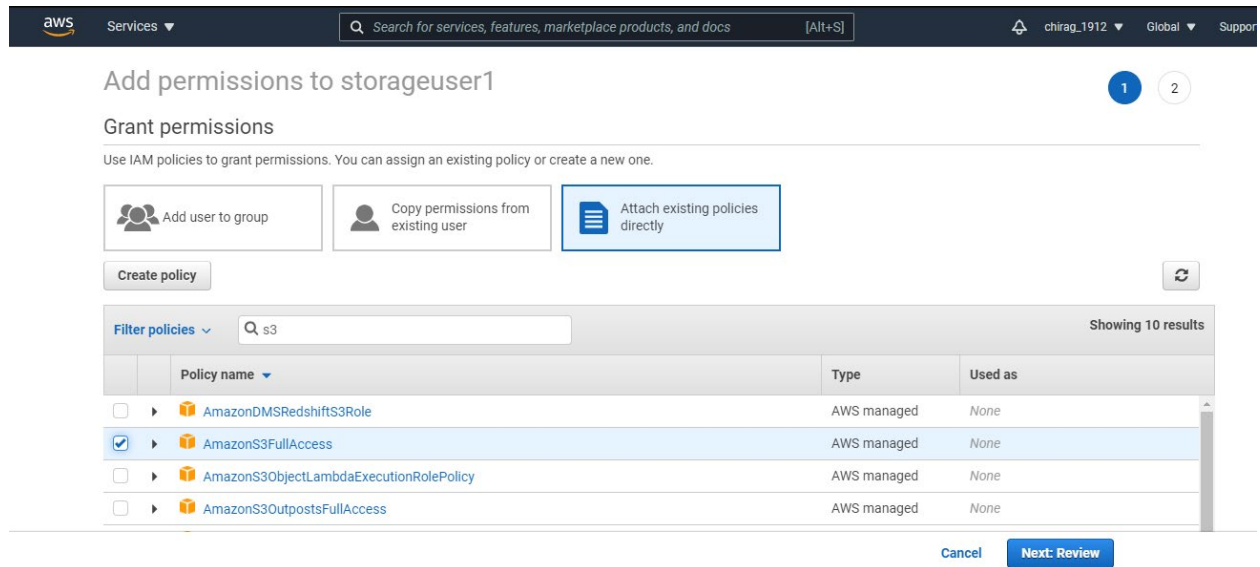
Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active
<input type="checkbox"/>	storageuser1	None	Never	None	✓ 19 minutes ago	-
<input type="checkbox"/>	storageuser2	None	Never	None	✓ 19 minutes ago	-

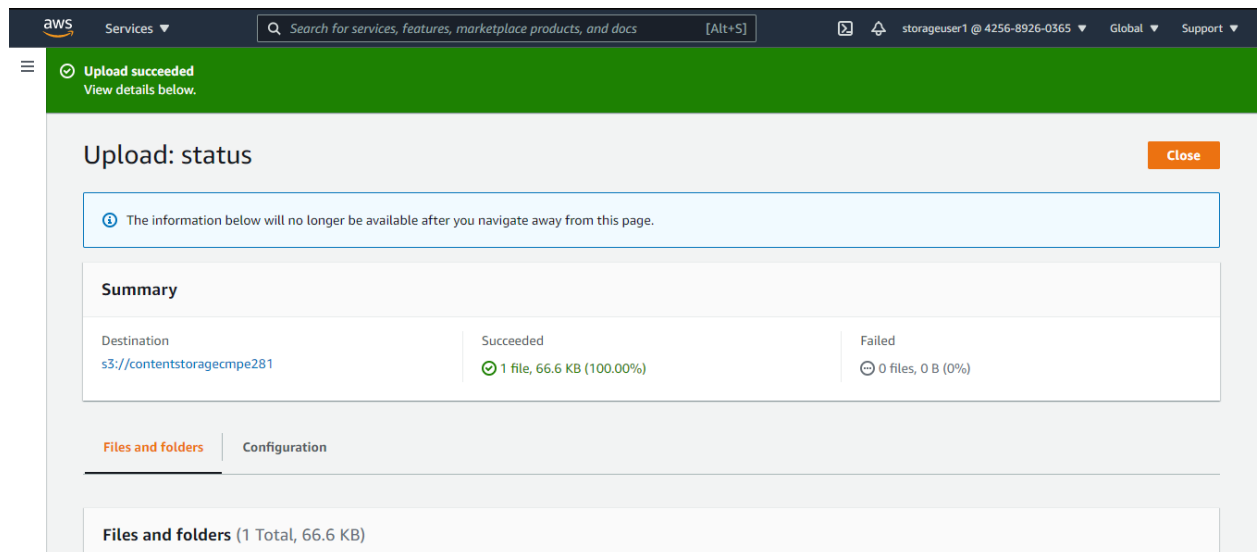
- Storage User 1 given permission S3 Full Access(including read/write). Which enables the user to upload and download the files from the S3 bucket for which the permission is granted.



The screenshot shows the AWS IAM console interface for adding permissions to a user named 'storageuser1'. The 'Grant permissions' section is active, and the 'AmazonS3FullAccess' policy is selected from the list of policies. The table below shows the list of policies available for selection.

Policy name	Type	Used as
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	None
<input checked="" type="checkbox"/> AmazonS3FullAccess	AWS managed	None
<input type="checkbox"/> AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	None

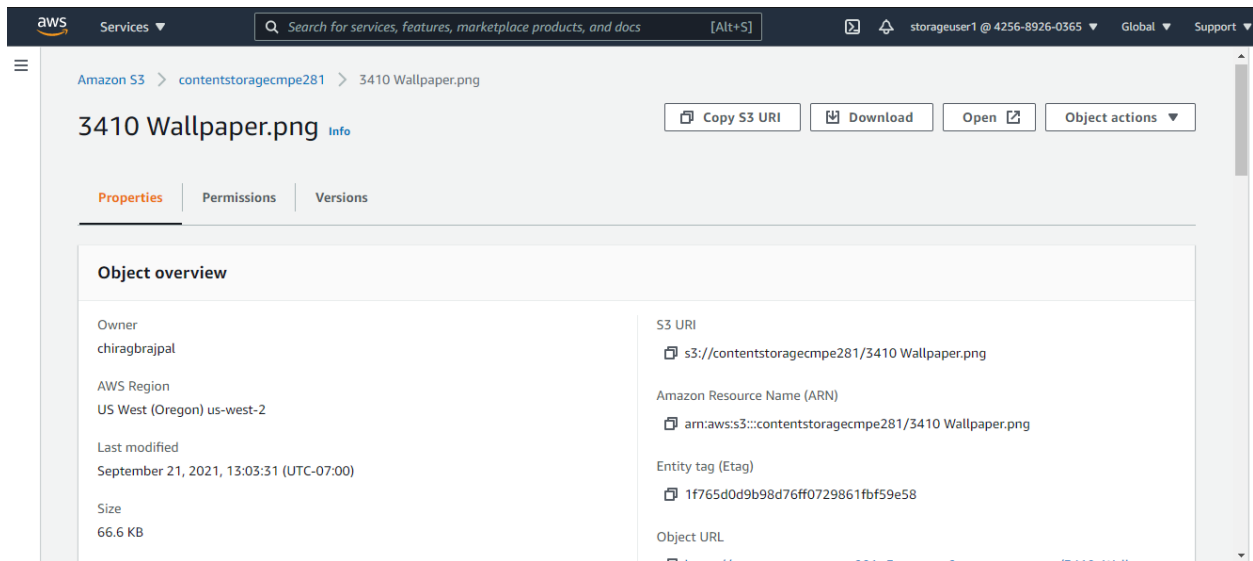
- Logging in with User1 to showcase user1 has full access for download/upload operations: File has been uploaded by the user1 to S3 bucket (storagecontainercmpe281).



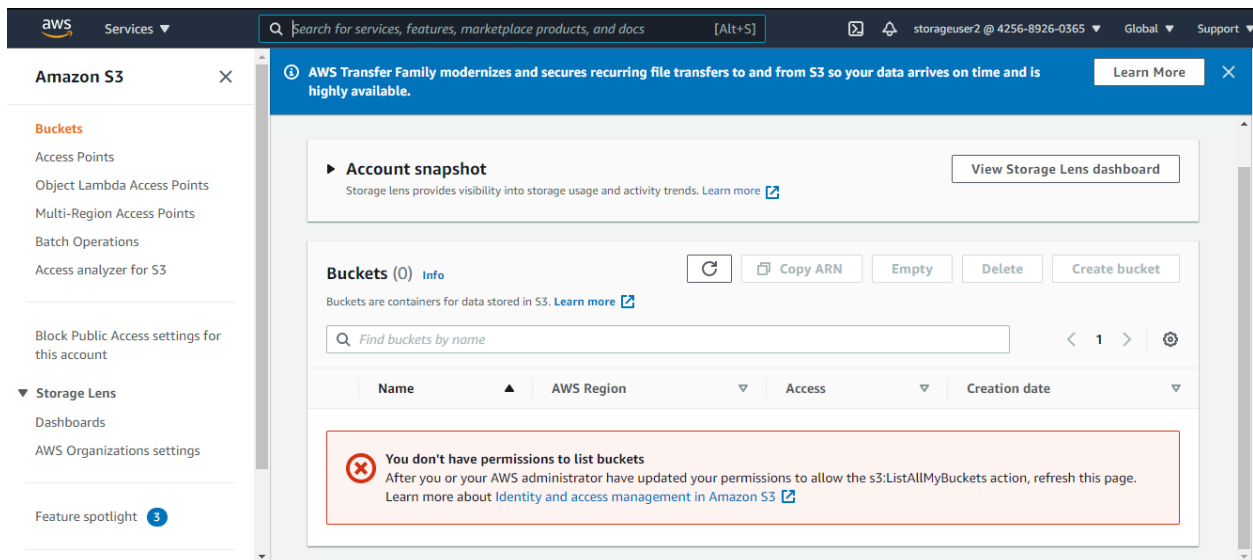
The screenshot shows the AWS S3 console interface for the 'Upload: status' page. The page displays a summary of the upload operation, indicating that 1 file (66.6 KB) was successfully uploaded to the S3 bucket s3://contentstoragecmpe281.

Destination	Succeeded	Failed
s3://contentstoragecmpe281	1 file, 66.6 KB (100.00%)	0 files, 0 B (0%)

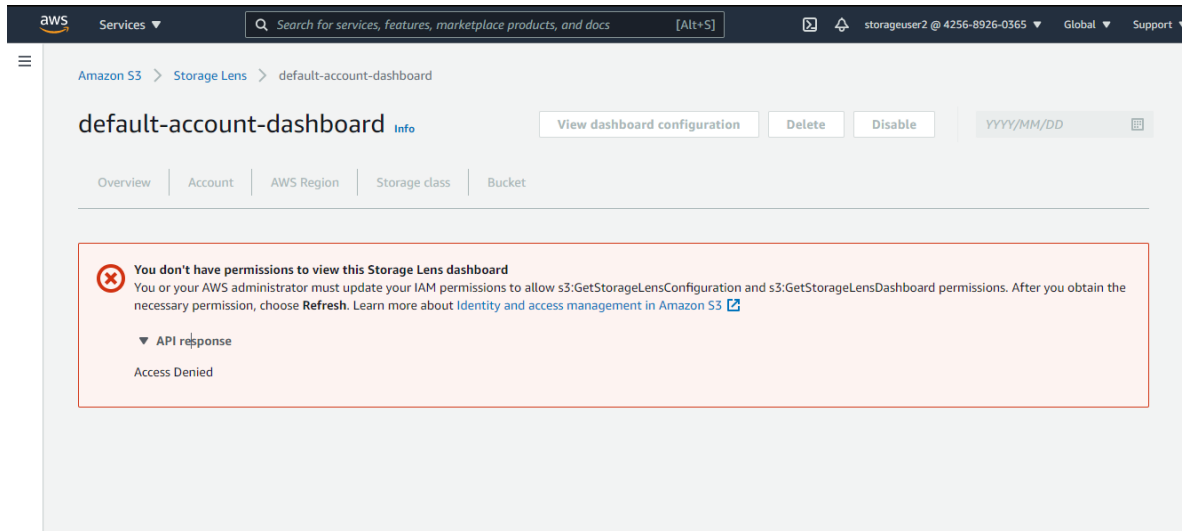
- Option for file download is visible and accessible to the first storage user1.



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

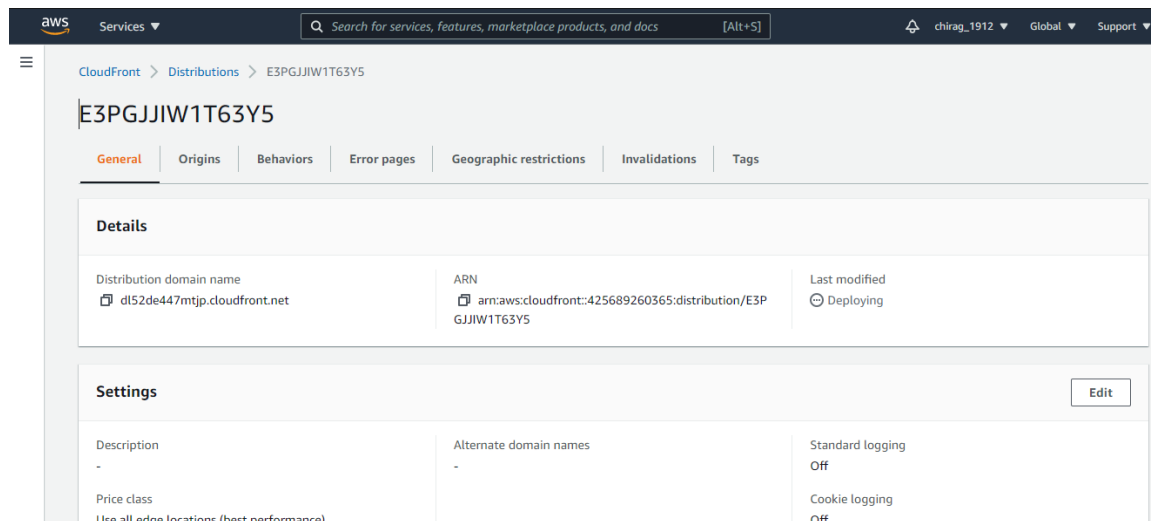


7. Permissions denied for the storageuser2 which is not given read/write permission in IAM:

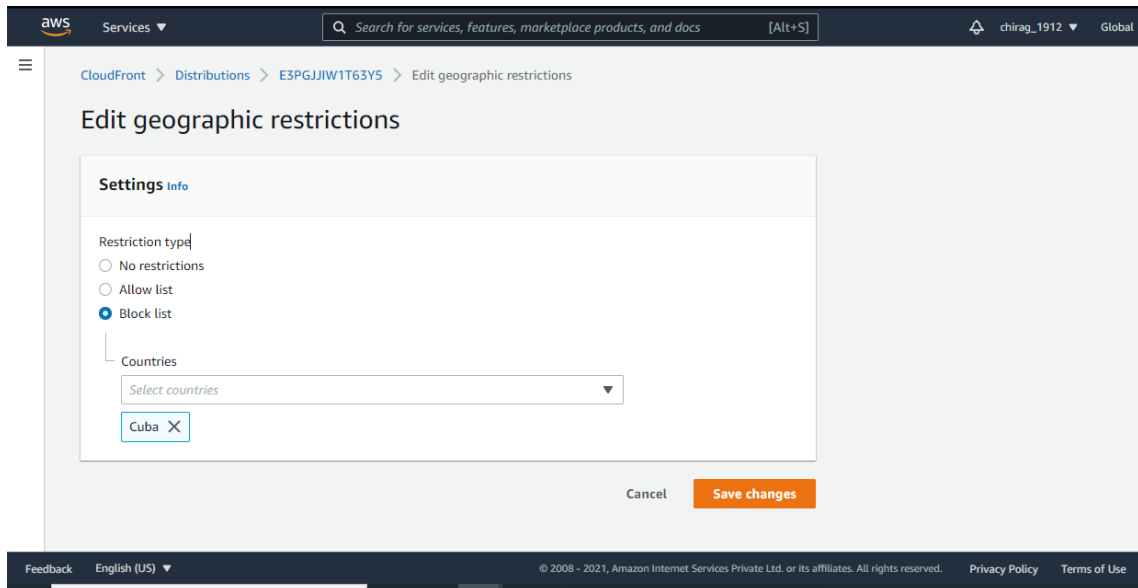


6. To block access of IP connections coming from a particular region:

1. Distribution(E3PGJJW1T63Y5) created in Cloud Front in order to block access.



2. Adding Blocklist for Cuba Territory 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:

