AWS - S3

What is Amazon S3?

- Amazon S3 stands for Simple Storage Service.
- It is cloud storage service provided by AWS
- S3 has characteristics -
    - Highly Scalable
    - Highly Available
    - Secure
    - Cost Effective
    - Performance
- It allows you to store and retrieve any amount of data from anywhere on the web.
- AWS S3 is also called as a version solution

What can you store in these S3?

- S3 services allows you to create buckets in which you can store everything.
    - Eg: we can store pictures, movies (or) any kind of files and folders (or) excel sheets etc..,
- But, as a DevOps Engineer What we will deal with is
    - Application log files, big databases, backup's, huge application supported configuration files etc..,
- Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IOT devices and big data analytics

What are S3 buckets?

S3 buckets are containers for storing objects (files) in Amazon S3. Each bucket has a unique name globally across all of AWS. You can think of an S3 bucket as a top-level folder that holds your data.

Buckets :

- Bucket is a component in S3
- If you create a folder in root level then it is called as buckets
- Buckets is used to store objects
- Bucket ownership is not transferrable to another account
- After we create a bucket, we can't change it's name (or) region
- We cannot delete the bucket directly. We need to make empty if first
- After a bucket is deleted, the name becomes available for reuse
- By default, we can create up to 100 buckets in each of your AWS account
- If you need additional buckets, you can increase your account bucket limit to 1,000 buckets by submitting a service limit increase

Objects :

- In bucket, you are storing the files is called objects
- To store your data in Amazon S3, you work with resources known as buckets and objects
- A bucket is a container for objects

- An object is a file and any metadata that describes that file
- With Amazon S3, you pay only for what you use.

Depending on the size of the data you are uploading, Amazon S3 offers the following options

- Upload an object with single operation using the AWS SDKs, REST API (or) AWS CLI
  - with single PUT operation, you can upload a single object up to 5GB in size
- Upload a single object using the Amazon S3 Console
  - With the Amazon S3 console, you can upload a single object up to 160 GB in size

Major Components Of Object :

- Key → name of the object. Eg: file.txt → key
- Value → Data in bytes. (file size)
- Version → Shows versioning ID for uniqueness of object
- Metadata → data about the data (or) it describes about the data

Why use S3 buckets?

- S3 buckets provide a reliable and highly scalable storage solution for various use cases.
- They are commonly used for backup and restore, data archiving, content storage for websites, and as a data source for big data analytics.
- It solves the storage problem for companies (or) organizations
- We can store the WAR files here
- Applications related log files generating purpose we can use S3
- Using S3 bucket we can host the website instead of EC2 instance
- Application contains some files. We can store that files here

We're using S3 instead of Nexus also, because maintenance easy in S3. and in nexus we need to do complex setup for that we need t2.medium, 20 GB volume, etc.., cost is high

S3 is globally accessible, we can access the data in s3 anywhere

What happened if S3 goes down ?

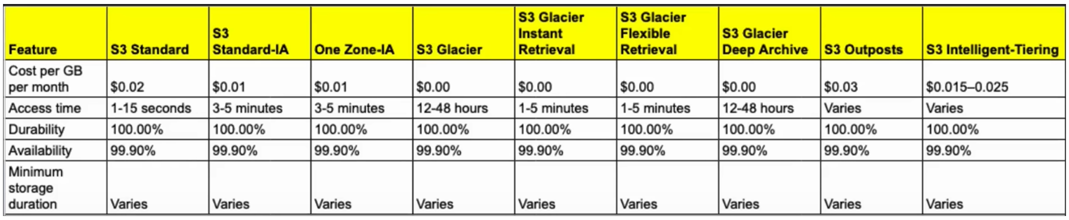
The Secret behind the success in S3 is → 11 (9's)

- 99.99999999999
  - It indicates the amount of reliability of AWS S3.
- i.e. when you upload a data in S3 and we thought like what if the data deleted/S3 down
  - So, S3 is giving the assurance like it giving the reliability to your objects
- So, that means in S3 our object will never gets deleted
  - Because of the replication mechanism of AWS
  - i.e. if you create an object S3 it will store your data in multiple availability zones. Every zone has some copies of your data. So, when you lose your data also, AWS have replicas. So, they can retrieve the data

Key Benefits of S3 buckets

S3 buckets offer several advantages, including:

- Durability and availability:
  - S3 provides high durability and availability for your data.
- Scalability:
  - You can store and retrieve any amount of data without worrying about capacity constraints.
- Security:
  - S3 offers multiple security features such as encryption, access control, and audit logging and bucket policies.
  - Encrypt data at rest using server-side encryption options provided by S3. Additionally, enable encryption in transit by using SSL/TLS for data transfers
  - Enable access logging to capture detailed records of requests made to your S3 bucket
  - Monitor access logs and configure alerts to detect any suspicious activities (or) unauthorized access attempts
- Performance:
  - S3 is designed to deliver high performance for data retrieval and storage operations.
  - If we create a S3 in the region that is near by us. then we can quickly access the content in S3. like you can upload (or) download the content in S3 very quickly
- Cost-effective:
  - S3 offers cost-effective storage options and pricing models based on your usage patterns.
  - It depends on the storage class patterns.
  - It depends on the type of data that you are storing and it depends on what your organization needs.
  - In the below image features are nothing but storage classes



Feature	S3 Standard	S3 Standard-IA	One Zone-IA	S3 Glacier	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive	S3 Outposts	S3 Intelligent-Tiering
Cost per GB per month	$0.02	$0.01	$0.01	$0.00	$0.00	$0.00	$0.00	$0.03	$0.015–0.025
Access time	1-15 seconds	3-5 minutes	3-5 minutes	12-48 hours	1-5 minutes	1-5 minutes	12-48 hours	Varies	Varies
Durability	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
Availability	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%	99.90%
Minimum storage duration	Varies	Varies	Varies	Varies	Varies	Varies	Varies	Varies	Varies

  - Eg: if we store 1TB data in S3 per one year. It will costs like 5 (or) 6 dollars.

Bucket properties and configurations

Versioning:

- Versioning allows you to keep multiple versions of an object in the bucket.
- It helps protect against accidental deletions or overwrites.

Bucket-level permissions and policies

Bucket-level permissions and policies define who can access and perform actions on the bucket. You can grant permissions using IAM (Identity and Access Management) policies, which allow fine-grained control over user access to the bucket and its objects.

Uploading and Managing Objects in S3 Buckets

Uploading objects to S3 buckets

You can upload objects to an S3 bucket using various methods, including the AWS Management Console, AWS CLI, SDKs, and direct HTTP uploads. Each object is assigned a unique key (name) within the bucket to retrieve it later.

Object metadata and properties

Object metadata contains additional information about each object in an S3 bucket. It includes attributes like content type, cache control, encryption settings, and custom metadata. These properties help in managing and organizing objects within the bucket.

File formats and object encryption

S3 supports various file formats, including text files, images, videos, and more. You can encrypt objects stored in S3 using server-side encryption (SSE). SSE options include SSE-S3 (Amazon-managed keys), SSE-KMS (AWS Key Management Service), and SSE-C (customer-provided keys).

Lifecycle management

Lifecycle management allows you to define rules for transitioning objects between different storage classes or deleting them automatically based on predefined criteria. For example, you can move infrequently accessed data to a lower-cost storage class after a specified time or delete objects after a certain retention period.

Multipart uploads

Multipart uploads provide a mechanism for uploading large objects in parts, which improves performance and resiliency. You can upload each part in parallel and then combine them to create the complete object. Multipart uploads also enable resumable uploads in case of failures.

Managing large datasets with S3 Batch Operations

S3 Batch Operations is a feature that allows you to perform bulk operations on large numbers of objects in an S3 bucket. It provides an efficient way to automate tasks such as copying objects, tagging, and restoring archived data.

Advanced S3 Bucket Features

S3 Storage Classes

S3 offers multiple storage classes, each designed for different use cases and performance requirements:

S3 Replication

S3 replication enables automatic and asynchronous replication of objects between S3 buckets in different regions or within the same region. Cross-Region Replication (CRR) provides disaster recovery and compliance benefits, while Same-Region Replication (SRR) can be used for data resilience and low-latency access.

S3 Event Notifications and Triggers

S3 event notifications allow you to configure actions when specific events occur in an S3 bucket. For example, you can trigger AWS Lambda functions, send messages to Amazon Simple Queue Service (SQS), or invoke other services using Amazon SNS when an object is created or deleted.

S3 Batch Operations

S3 Batch Operations allow you to perform large-scale batch operations on objects, such as copying, tagging, or deleting, across multiple buckets. It simplifies managing large datasets and automates tasks that would otherwise be time-consuming.

Security and Compliance in S3 Buckets

- S3 bucket security considerations
  - Ensure that S3 bucket policies, access control, and encryption settings are appropriately configured.
  - Regularly monitor and audit access logs for unauthorized activities.
- Data encryption at rest and in transit
  - Encrypt data at rest using server-side encryption options provided by S3.
  - Additionally, enable encryption in transit by using SSL/TLS for data transfers.
- Access logging and monitoring
  - Enable access logging to capture detailed records of requests made to your S3 bucket.
  - Monitor access logs and configure alerts to detect any suspicious activities or unauthorized access attempts.

S3 Bucket Management and Administration

- S3 bucket policies
  - Create and manage bucket policies to control access to your S3 buckets.
  - Bucket policies are written in JSON and define permissions for various actions and resources.
- S3 access control and IAM roles
  - Use IAM roles and policies to manage access to S3 buckets.
  - IAM roles provide temporary credentials and fine-grained access control to AWS resources.
- S3 APIs and SDKs
  - Interact with S3 programmatically using AWS SDKs or APIs.
  - These provide libraries and methods for performing various operations on S3 buckets and objects.
- Monitoring and logging with CloudWatch
  - Utilize Amazon CloudWatch to monitor S3 metrics, set up alarms for specific events, and collect and analyze logs for troubleshooting and performance optimization.
- S3 management tools
  - AWS provides multiple management tools, such as the AWS Management Console, AWS CLI, and third-party tools, to manage S3 buckets efficiently and perform operations like uploads, downloads, and bucket configurations.

Troubleshooting and Error Handling

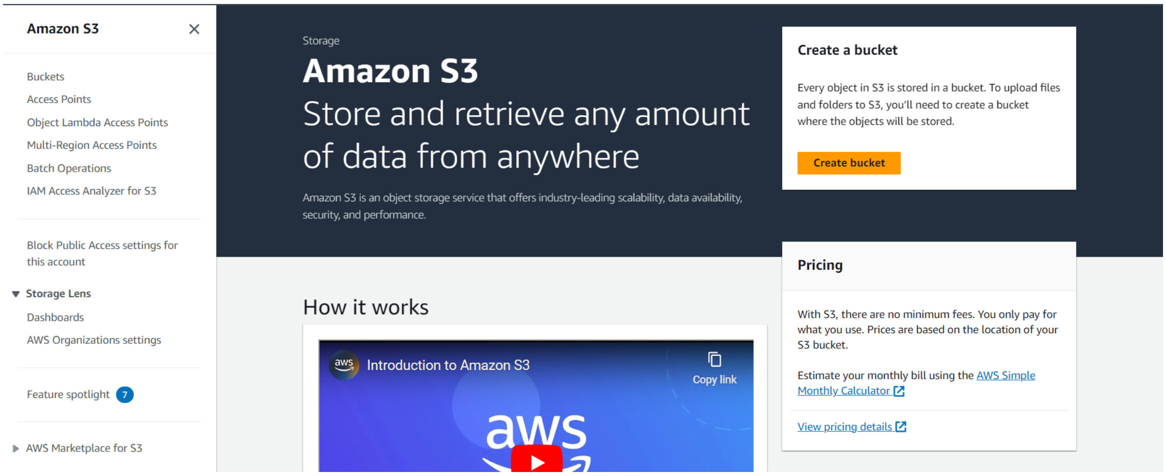
- Common S3 error messages and their resolutions
  - Understand common S3 error messages like access denied, bucket not found, and exceeded bucket quota.

    - Troubleshoot and resolve these errors by checking permissions, bucket configurations, and network connectivity.
- Debugging S3 bucket access issues
    - Investigate and resolve issues related to access permissions, IAM roles, and bucket policies.
    - Use tools like AWS CloudTrail and S3 access logs to identify and troubleshoot access problems.
- Data consistency and durability considerations
    - Ensure data consistency and durability by understanding S3's data replication and storage mechanisms.
    - Verify that data is correctly uploaded, retrieve objects using proper methods, and address any data integrity issues.
- Recovering deleted objects
    - If an object is accidentally deleted, you can often recover it using versioning or S3 event notifications.
    - Additionally, consider enabling Cross-Region Replication (CRR) for disaster recovery scenarios.

Creating and Configuring S3 Buckets

Practice - DeepDive

Go to AWS → search S3 service → open → you get dashboard → click on create bucket



Amazon S3 ×

Buckets
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
AWS Organizations settings

Feature spotlight 7

▶ AWS Marketplace for S3

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

How it works

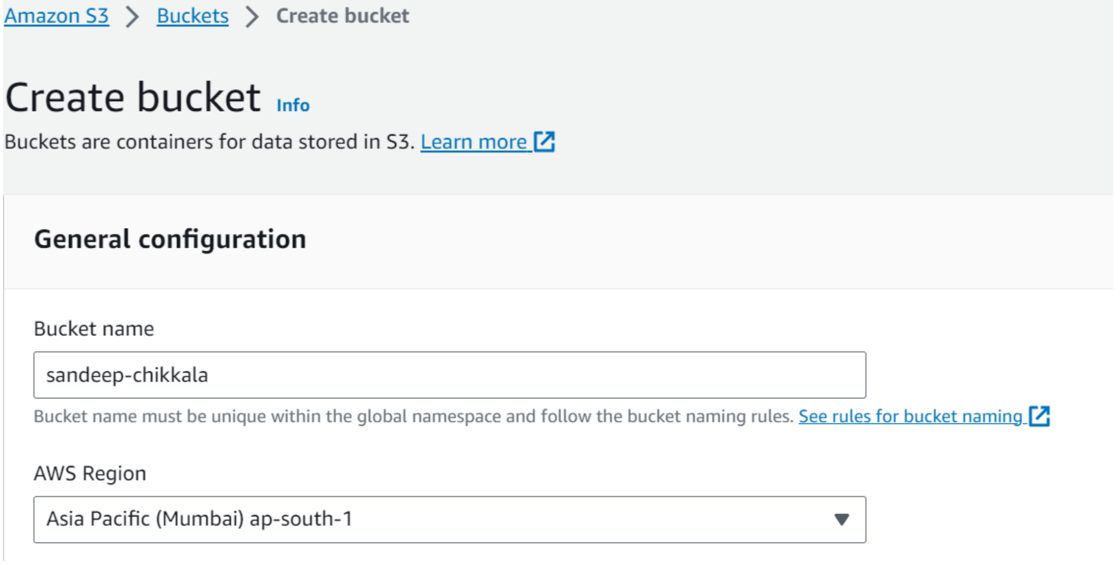
Creating an S3 bucket

- To create an S3 bucket, you can use the AWS Management Console, AWS CLI (Command Line Interface), or AWS SDKs (Software Development Kits).
- You need to specify a globally unique bucket name because it is globally accessing and select the region where you want to create the bucket.

Choosing a bucket name and region

- The bucket name must be unique across all existing bucket names in Amazon S3.
- It should follow DNS naming conventions, be 3-63 characters long, and contain only lowercase letters, numbers, periods, and hyphens.
- The region selection affects data latency and compliance with specific regulations.
- We are having regions, here we are choosing the nearest region due to latency issues
    - when I send a request to AWS, it has to cross multiple routers and it will reach data center and again I will get the request from AWS.

- ○ So, usually if my region is Mumbai means, it's very near for me.
- ○ To Solve the latency issues, we have to use region
- ○ Any resource that you are creating on AWS are bound to region



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

sandeep-chikkala

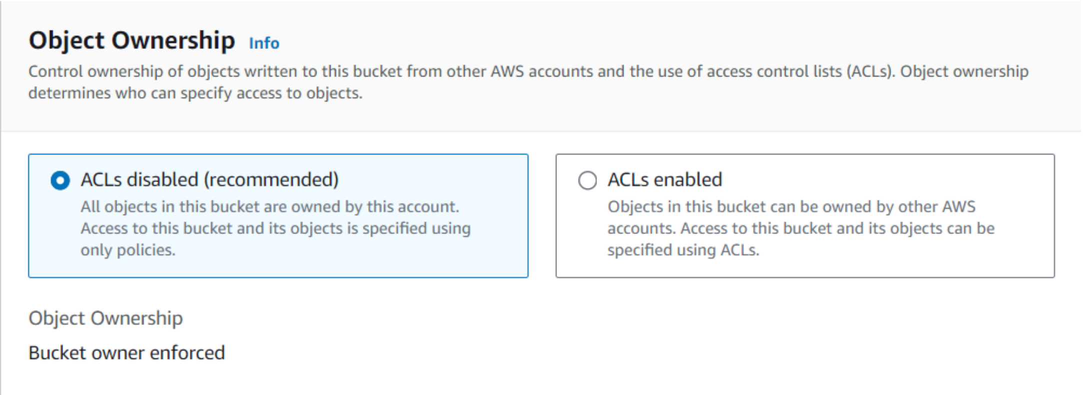
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

AWS Region

Asia Pacific (Mumbai) ap-south-1 ▼

Object Ownership

- Objects can be accessed by only you means, select ACL disabled
- Objects can be accessible to all means, select ACL enabled



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

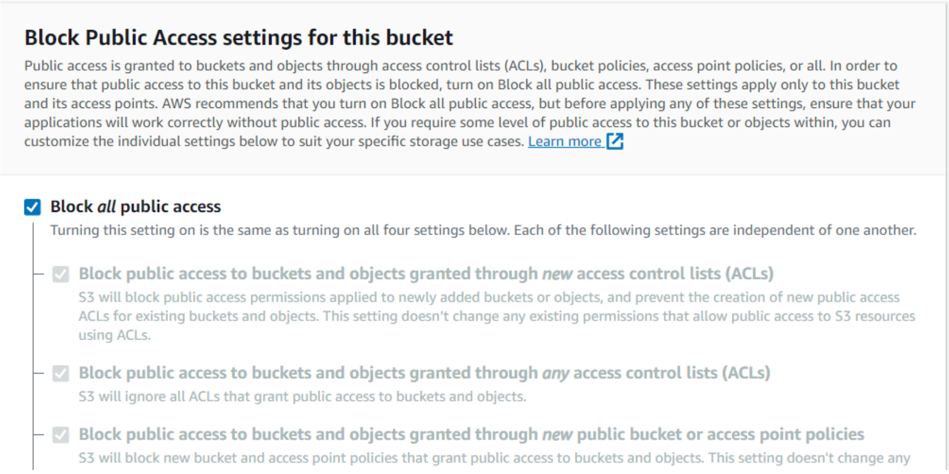
○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public access

- Inside bucket objects will be access to outside, uncheck the block all public access



Block Public Access settings for this bucket

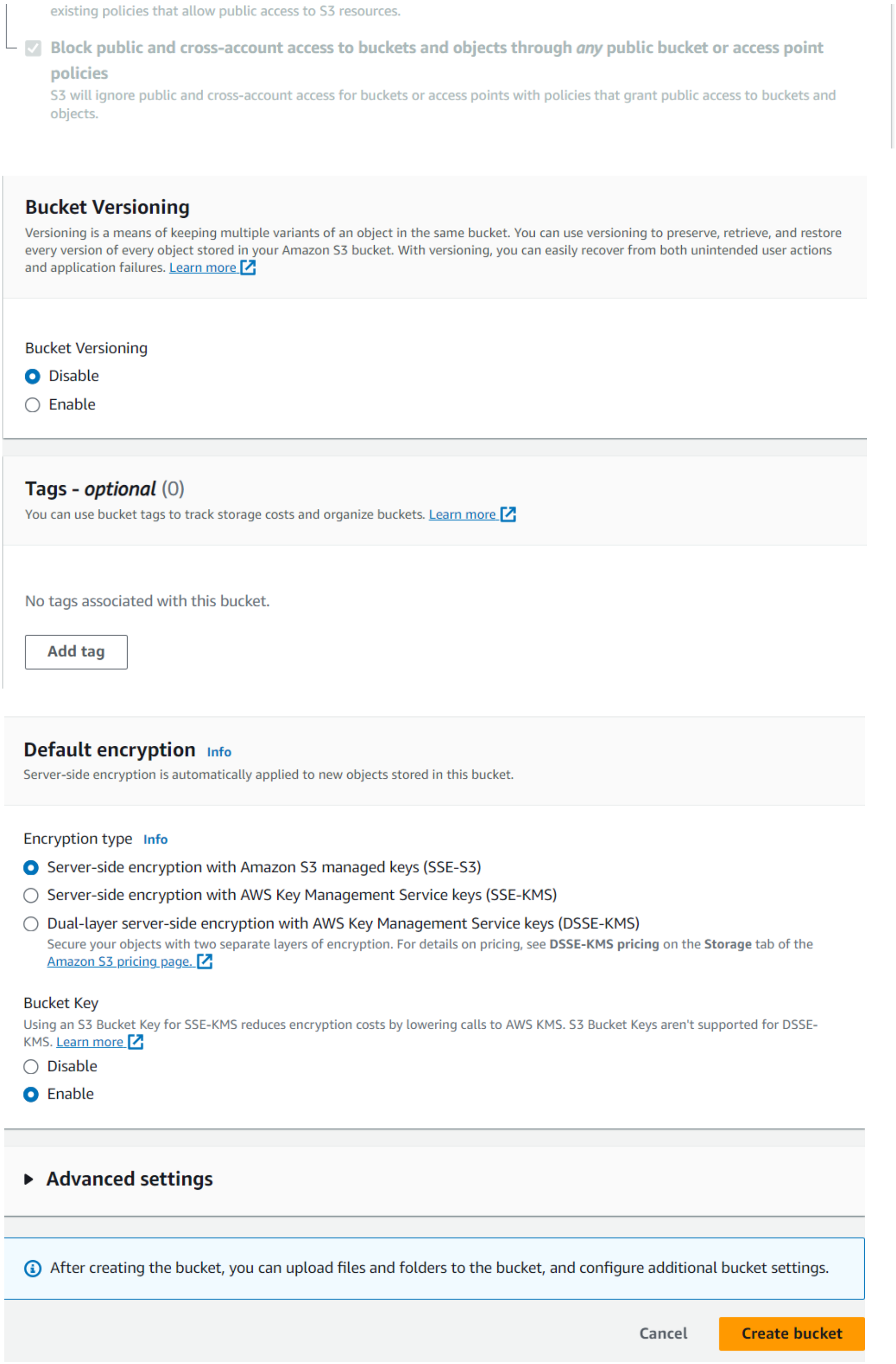
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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 this bucket 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.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
● Disable
○ Enable

Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

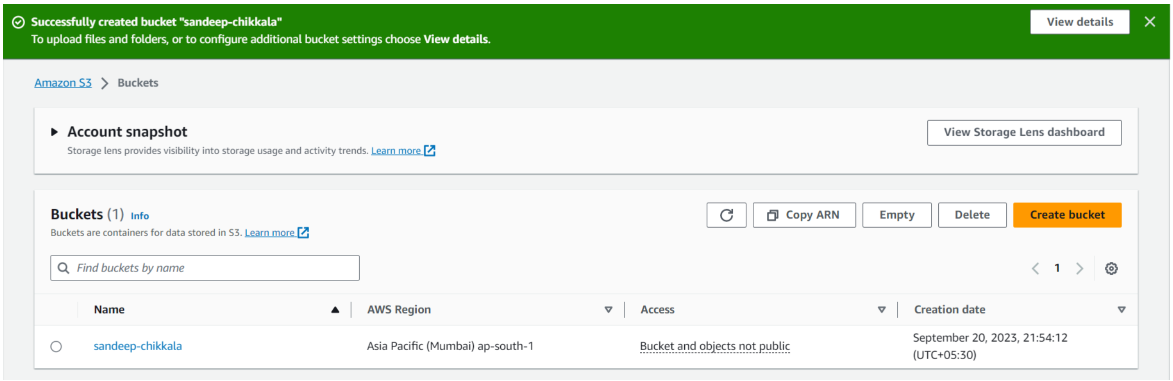
Encryption type Info
● Server-side encryption with Amazon S3 managed keys (SSE-S3)
○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
○ Disable
● Enable

▶ **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Once, click on Create bucket, you will get the below dashboard



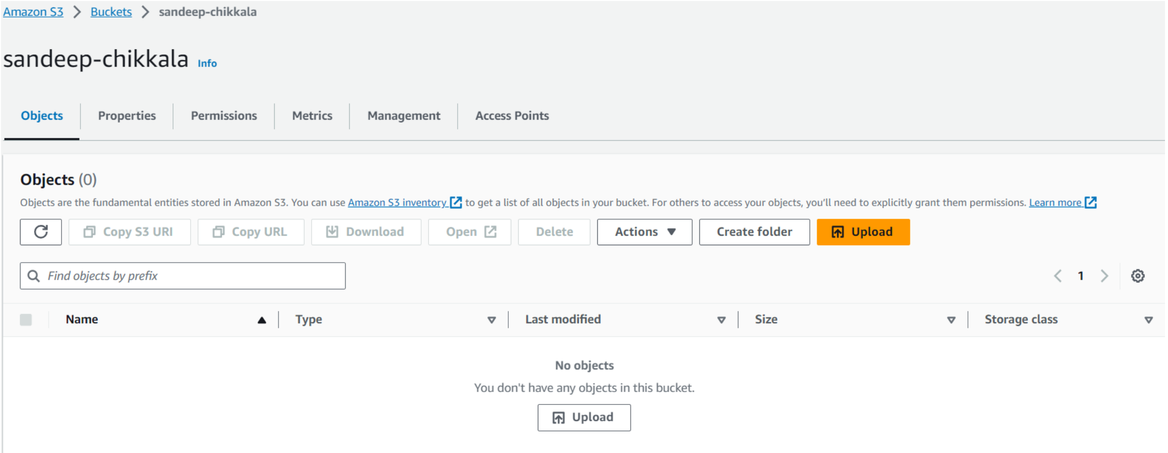
Successfully created bucket "sandeep-chikkala"
To upload files and folders, or to configure additional bucket settings choose **View details**.

▶ **Account snapshot**
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info
Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	sandeep-chikkala	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	September 20, 2023, 21:54:12 (UTC+05:30)

- Click on the bucket name, you will get below image

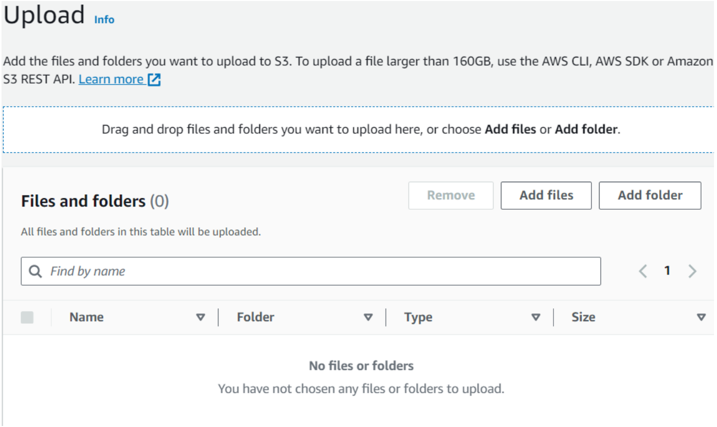


Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects

You don't have any objects in this bucket.

  - when you click on the bucket, usually you can see objects. Present we don't have objects
  - so, click on upload, you can click on add files and upload the data from your local
  - At a time, multiple files & folders also we can upload.



Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

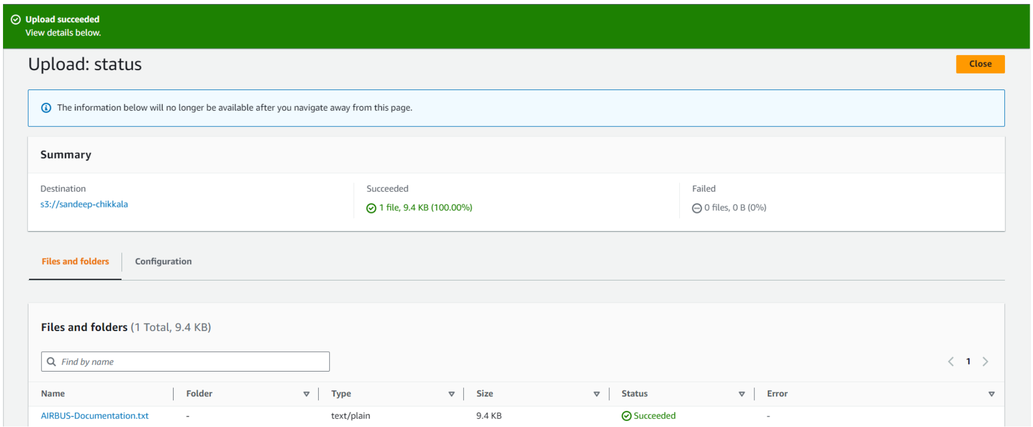
Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

All files and folders in this table will be uploaded.

No files or folders

You have not chosen any files or folders to upload.

- After successfully uploaded, you will get below image



Upload succeeded

View details below.

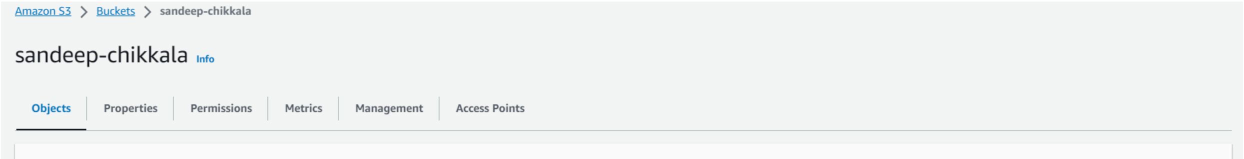
The information below will no longer be available after you navigate away from this page.

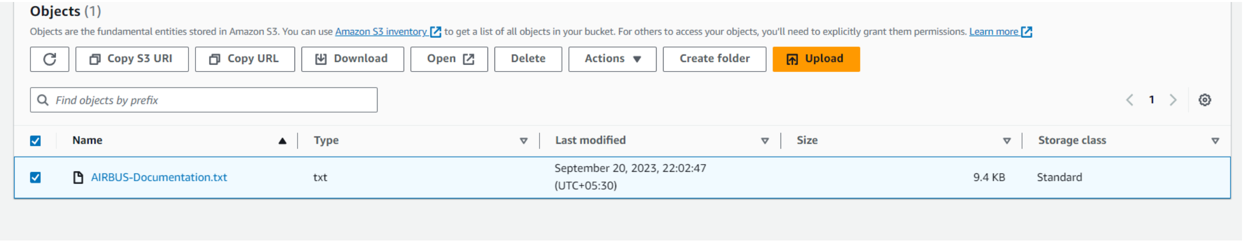
Destination	Succeeded	Failed
s3://sandeep-chikkala	1 file, 9.4 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 9.4 KB)

Name	Folder	Type	Size	Status	Error
AIRBUS-Documentation.txt	-	text/plain	9.4 KB	Succeeded	-

- After uploaded the files in the bucket, you will have the objects. If you select that fileg, you will get below image

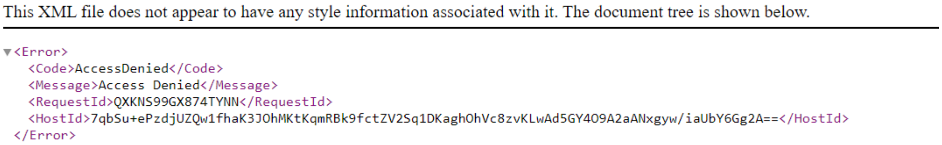




Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	Last modified	Size	Storage class
☑	AIRBUS-Documentation.txt	txt	September 20, 2023, 22:02:47 (UTC+05:30)	9.4 KB	Standard

- If you select a file we're getting so many options
- Copy S3 URI → it contains file path → s3://sandeep-chikkala/AIRBUS-Documentation.txt
- Copy URL → It contains Bucket related URL
  - https://sandeep-chikkala.s3.ap-south-1.amazonaws.com/AIRBUS-Documentation.txt
  - when you access this URL in browser, you will get permission denied. Because, security is high for this



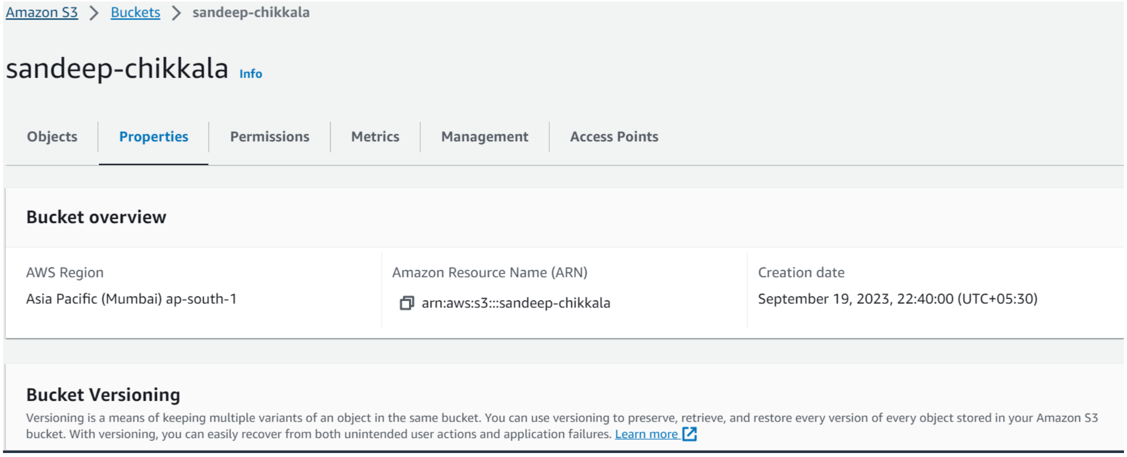
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>QXKNS99GX874TYNN</RequestId>
   <HostId>7qbSu+ePzdjUZQw1fhaK3JOhMKtKqmRBk9fctZV2Sq1DKaghOhVc8zvKLwAd5GY4O9A2aANxgyw/iaUbY6Gg2A==</HostId>
 </Error>
```

- Open → when you click on open, you will see the file output in browser
- Delete → we can delete the object file

If you want to delete a entire bucket, First, we need to empty the bucket. i.e. inside objects/files we have to delete, then after delete the bucket

□ When you opened a bucket, we're having properties



Bucket overview

AWS Region
Asia Pacific (Mumbai) ap-south-1

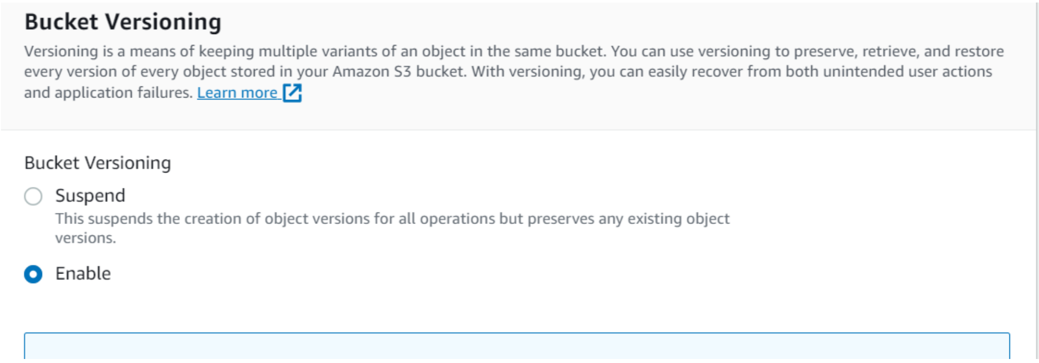
Amazon Resource Name (ARN)
arn:aws:s3:::sandeep-chikkala

Creation date
September 19, 2023, 22:40:00 (UTC+05:30)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

- If you want to enable the version, click on edit



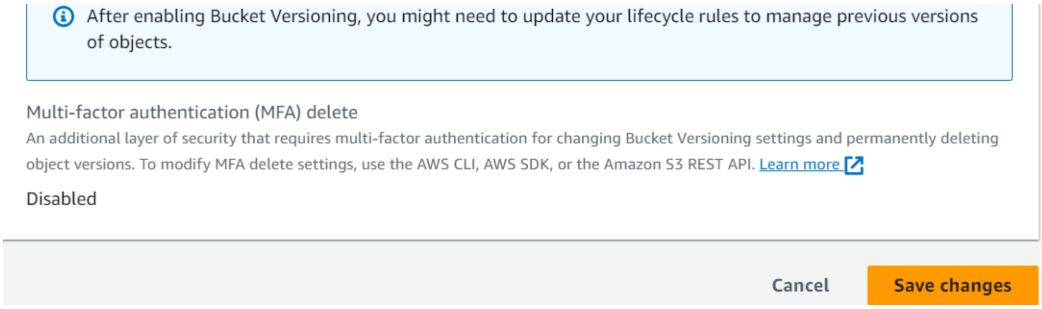
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

● Enable



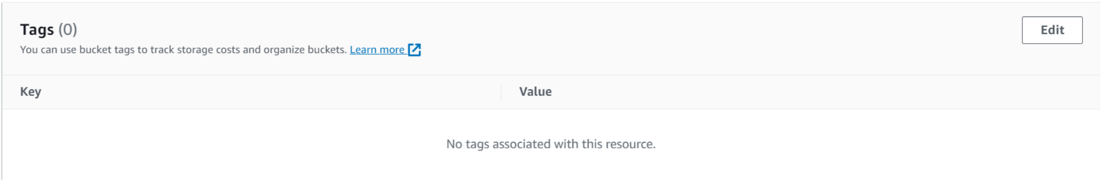
After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Disabled

- Tags is used for identifying the resources



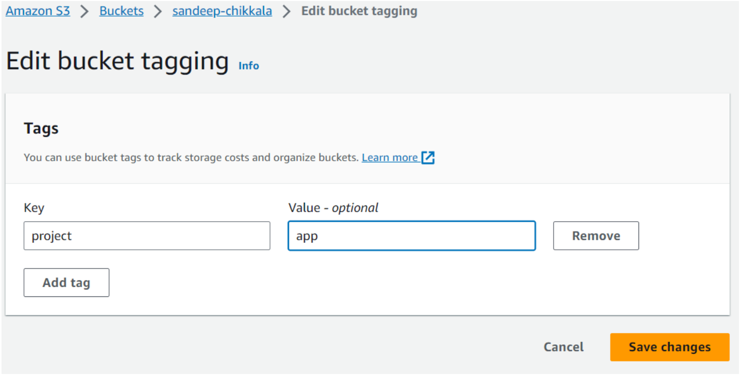
Tags (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

Key	Value

No tags associated with this resource.

  - click on edit, and add the data like below image



Amazon S3 > Buckets > sandeep-chikkala > Edit bucket tagging

Edit bucket tagging Info

Tags

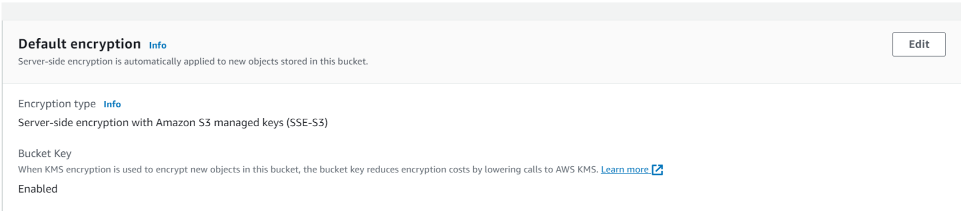
You can use bucket tags to track storage costs and organize buckets. Learn more

Key: project

Value - *optional*: app

  - when exactly, we will use means let's say we having multiple ec2, buckets across the world. If someone says that hey can you give me a list of S3 buckets that is used by this specific project then we can make use of this tags to identifying purpose
  - Every organization or every project that you are working with they have to create tags for sure and that way it will be easy for us to extract

Default Encryption



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

Server-side encryption with Amazon S3 managed keys (SSE-S3)

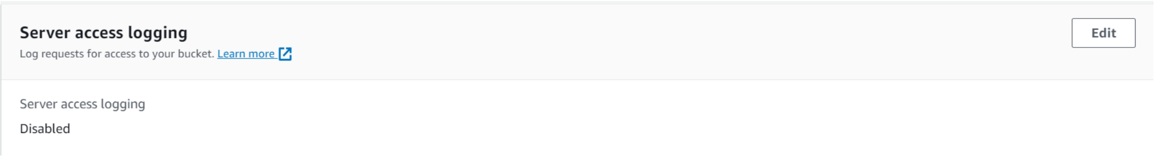
Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more

Enabled

  - S3 recently added the default encryption. Previously, you should have enabled the encryption on the objects but now the bucket encryption is available by default

Server Access Logging



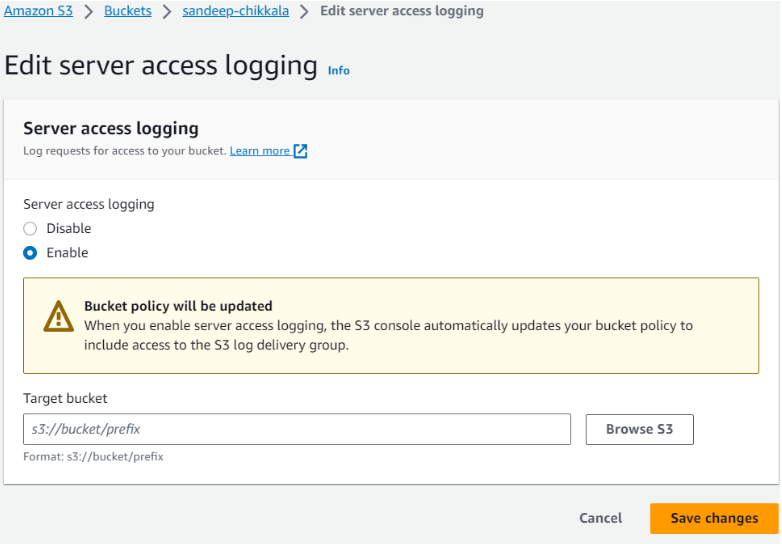
Server access logging

Log requests for access to your bucket. Learn more

Server access logging

Disabled

- We can enable this access logging by default this is disabled
- If you enable the access logging then it will ask like should be the policy here and then you can enable this access logging to ensure, who is logging into this bucket uh what kind of actions they are performing



Amazon S3 > Buckets > sandeep-chikkala > Edit server access logging

Edit server access logging Info

Server access logging

Log requests for access to your bucket. Learn more

Server access logging

○ Disable

● Enable

Bucket policy will be updated

When you enable server access logging, the S3 console automatically updates your bucket policy to include access to the S3 log delivery group.

Target bucket

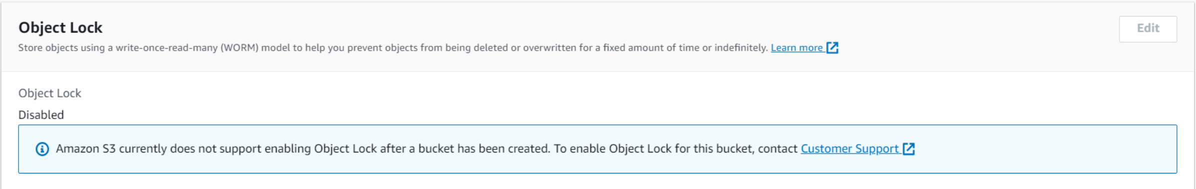
s3://bucket/prefix

Format: s3://bucket/prefix

- we can restrict also
- We can remove their access and we can send out the notifications depending upon the actions that they are performing

Object Locking

- once we upload the object into the bucket. I want to lock the object so that nobody else should use that object and that is locked there should not be any updates to the object right
- If someone wants to update the object then they cannot update the object probably some sensitive information which you have decided that nobody has to override then you can use the bucket locking



Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more

Object Lock

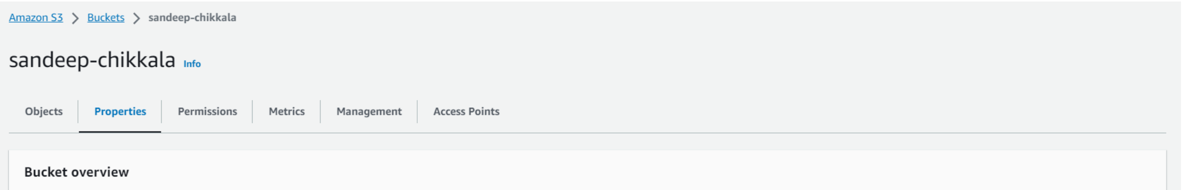
Disabled

Amazon S3 currently does not support enabling Object Lock after a bucket has been created. To enable Object Lock for this bucket, contact Customer Support

Enable the Version

How to enable the version for created bucket ?

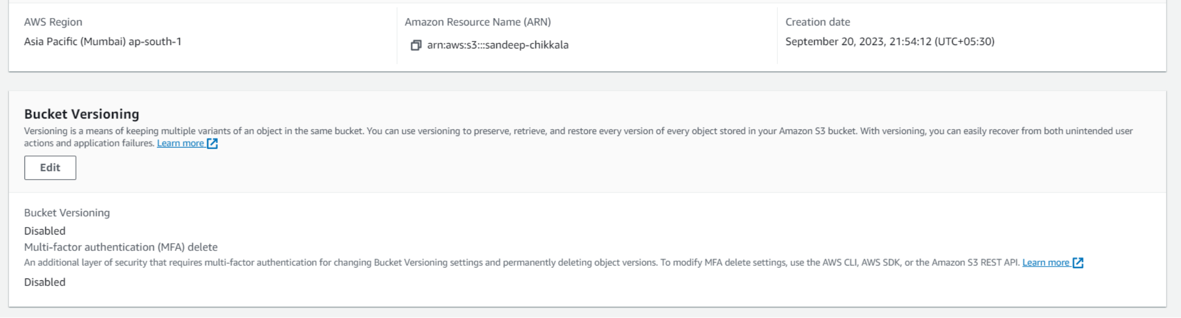
- click on bucket → properties



Amazon S3 > Buckets > sandeep-chikkala

sandeep-chikkala Info

Bucket overview



AWS Region
Asia Pacific (Mumbai) ap-south-1

Amazon Resource Name (ARN)
arn:aws:s3:::sandeep-chikkala

Creation date
September 20, 2023, 21:54:12 (UTC+05:30)

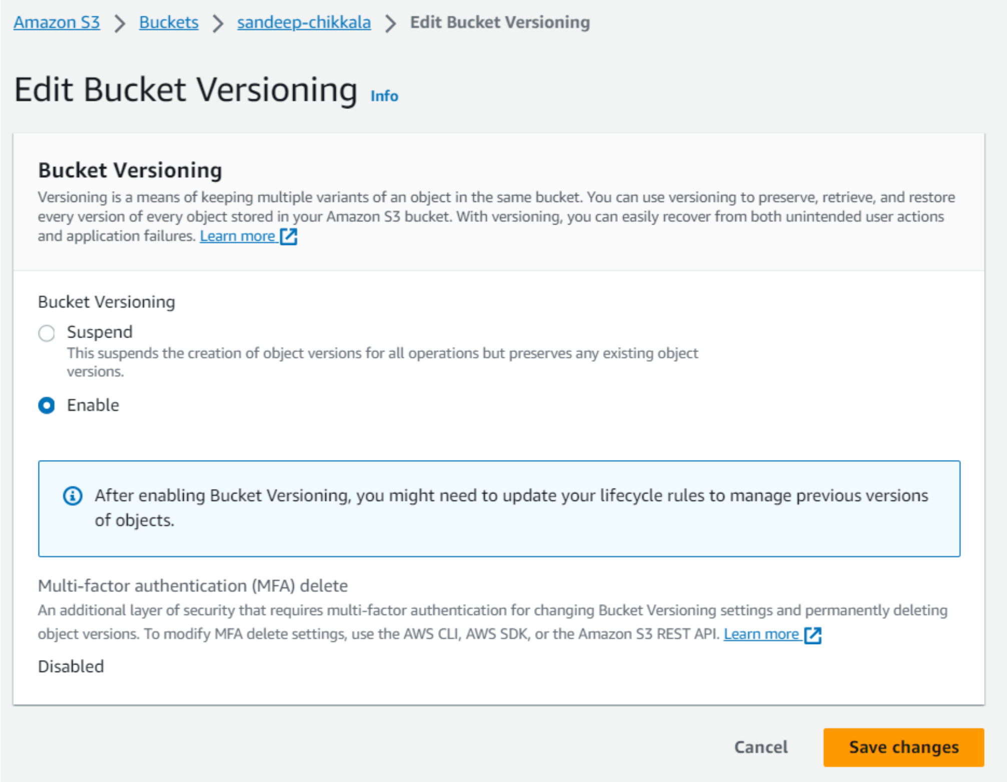
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

- **Now, go to Bucket Versioning → click on edit → click on enable → save**



Amazon S3 > Buckets > sandeep-chikkala > Edit Bucket Versioning

Edit Bucket Versioning Info

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

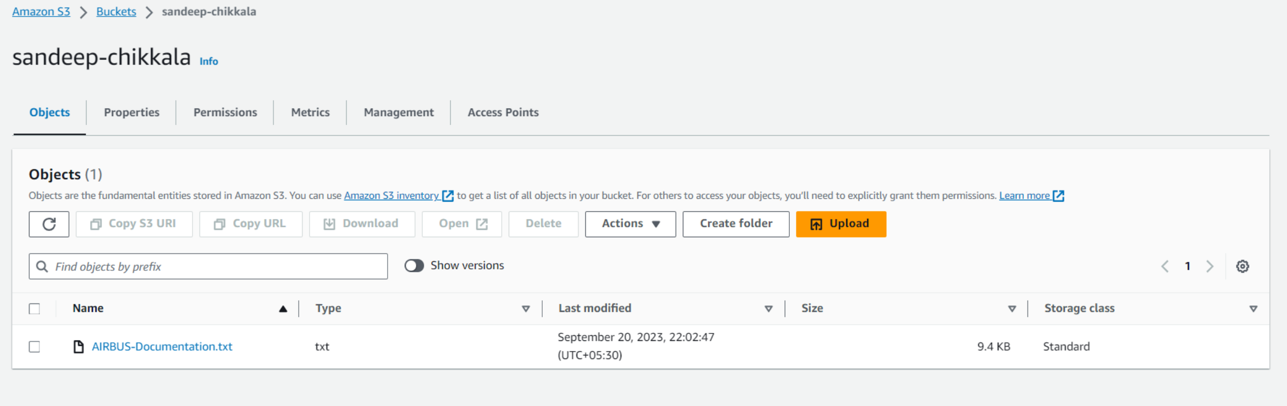
● Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Disabled

Now, when you go to buckets, you can see the "Show versions" in below image



Amazon S3 > Buckets > sandeep-chikkala

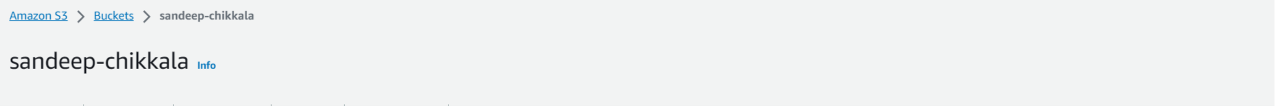
sandeep-chikkala Info

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

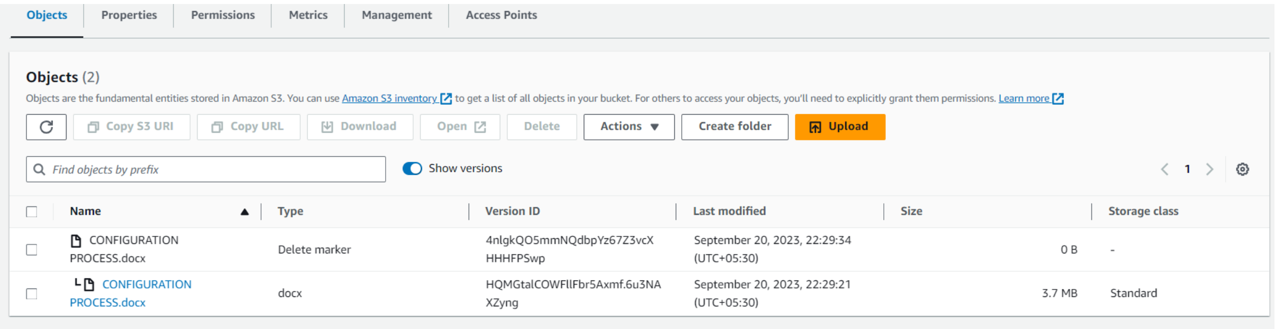
□	Name ▲	Type	Last modified	Size	Storage class
□	AIRBUS-Documentation.txt	txt	September 20, 2023, 22:02:47 (UTC+05:30)	9.4 KB	Standard

- **Now, when you delete the file means, it will deleted. But, when you enable the show versions, you can get the files like below image**



Amazon S3 > Buckets > sandeep-chikkala

sandeep-chikkala Info

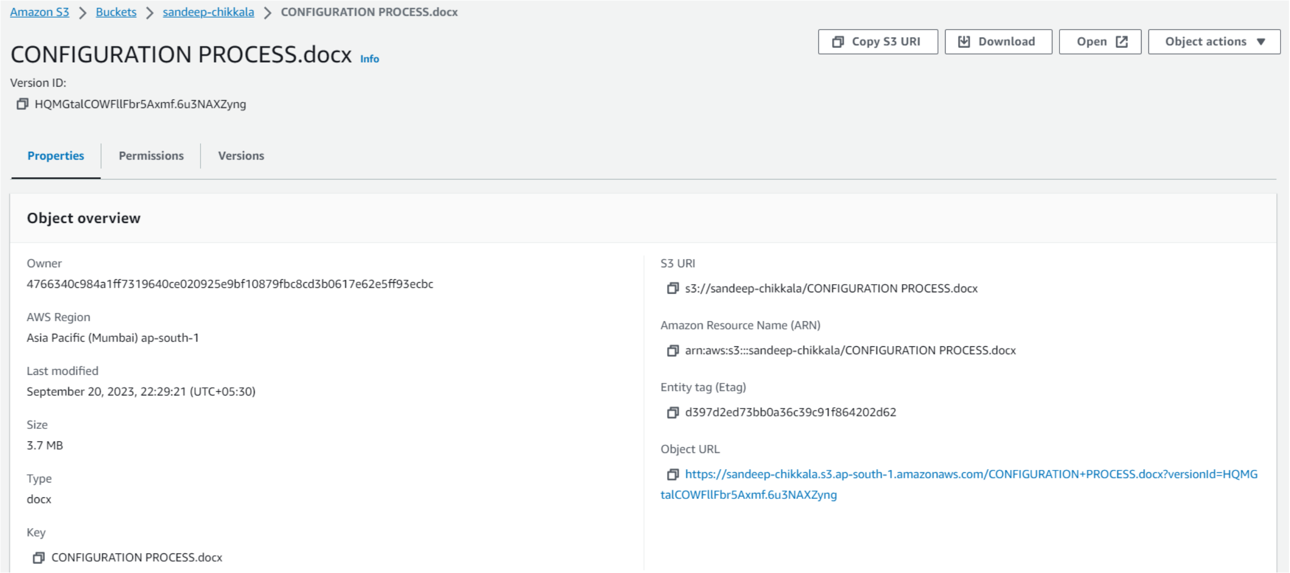


Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Version ID	Last modified	Size	Storage class
□	CONFIGURATION PROCESS.docx	Delete marker	4nlgkQO5mmNQdbpYz67Z3vcXHHHFPSwp	September 20, 2023, 22:29:34 (UTC+05:30)	0 B	-
□	CONFIGURATION PROCESS.docx	docx	HQMGtalCOWFllFbr5Axmf.6u3NAXZyng	September 20, 2023, 22:29:21 (UTC+05:30)	3.7 MB	Standard

- Now, when you click on the "standard" file in storage class i.e. 2nd one, you will get below image



CONFIGURATION PROCESS.docx

Version ID:
HQMGtalCOWFllFbr5Axmf.6u3NAXZyng

Object overview

Owner
4766340c984a1ff7319640ce020925e9bf10879fbc8cd3b0617e62e5ff93ecbc

AWS Region
Asia Pacific (Mumbai) ap-south-1

Last modified
September 20, 2023, 22:29:21 (UTC+05:30)

Size
3.7 MB

Type
docx

Key
CONFIGURATION PROCESS.docx

S3 URI
s3://sandeep-chikkala/CONFIGURATION PROCESS.docx

Amazon Resource Name (ARN)
arn:aws:s3:::sandeep-chikkala/CONFIGURATION PROCESS.docx

Entity tag (Etag)
d397d2ed73bb0a36c39c91f864202d62

Object URL
https://sandeep-chikkala.s3.ap-south-1.amazonaws.com/CONFIGURATION+PROCESS.docx?versionId=HQMGtalCOWFllFbr5Axmf.6u3NAXZyng

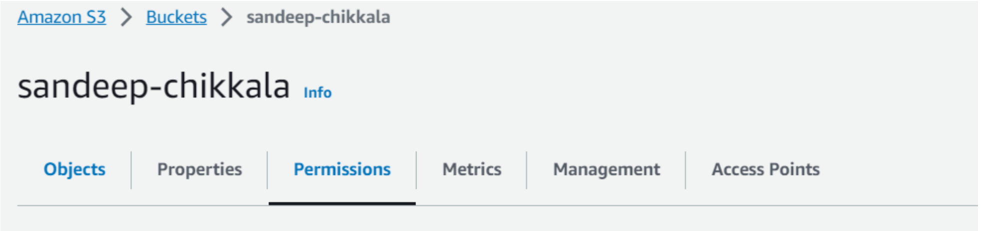
  - here, if you click on download, file will downloaded. And you can upload the file again

And when you're enable the versions, It will keep the multiple versions of the single file

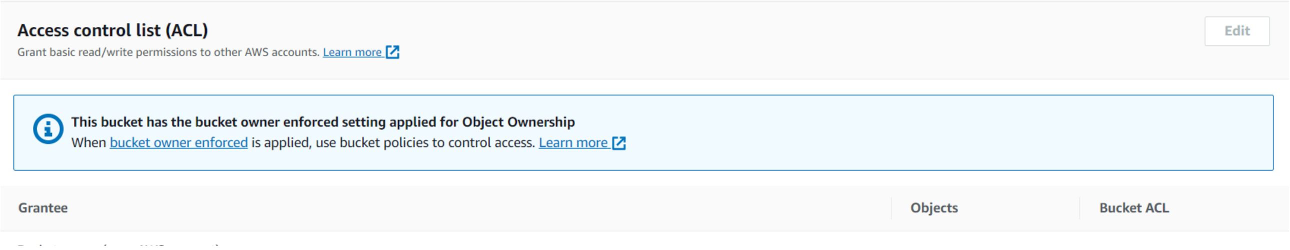
- For ex: if you upload the same file, multiple times it will track every file

Enable the Object Ownership

- Here, we are enabling the ownership for created bucket



- Now, go to permissions → Go to ACL

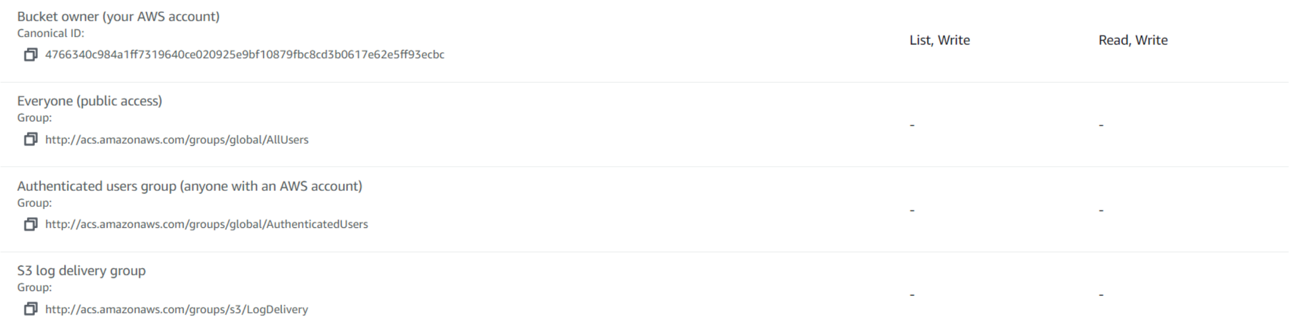


Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

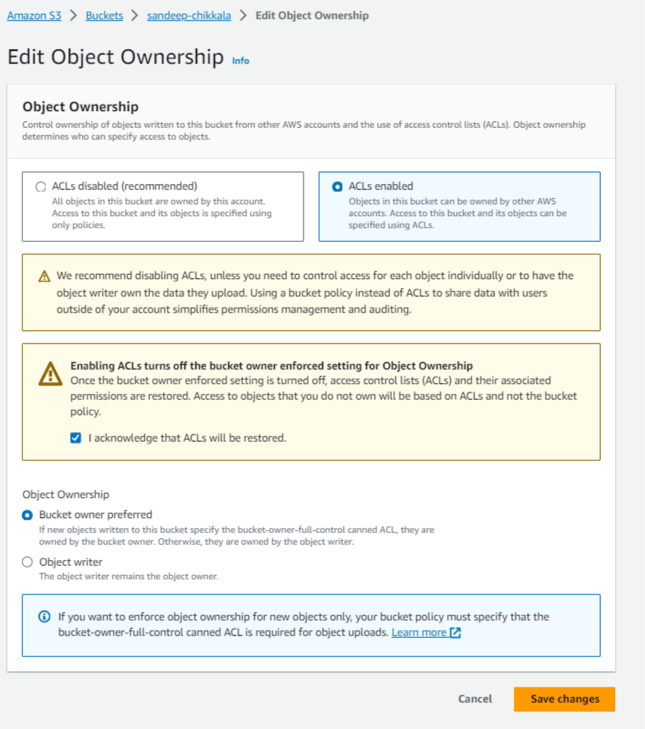
This bucket has the bucket owner enforced setting applied for Object Ownership
When bucket owner enforced is applied, use bucket policies to control access. Learn more

Grantee	Objects	Bucket ACL



Bucket owner (your AWS account) Canonical ID: 4766340c984a1ff7319640ce020925e9bf10879fbc8cd3b0617e62e5ff93ecbc	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

- Here, click on "bucket owner enforced"



Amazon S3 > Buckets > sandeep-chikkala > Edit Object Ownership

Edit Object Ownership Info

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

⚠ **Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**
Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☑ I acknowledge that ACLs will be restored.

Object Ownership

● Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

○ Object writer
The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

Advantages of Ownership

- If you enabled the ACL, previously when you're accessing the Copy URL from the object. It is showing permission denied error
- But, you enabled the ACL means, it will be open to all. So, people can read the file

CRR (Cross Region Replication)

If we upload the file in one bucket, that file will goes to another bucket,

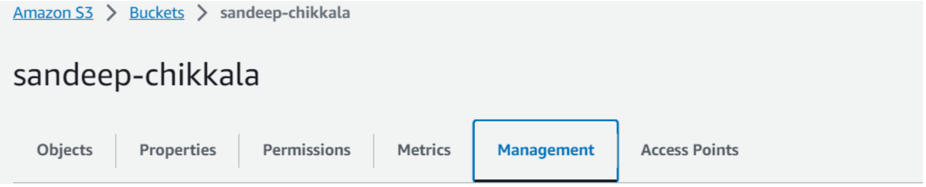
Step - 1:

- Create 2 buckets, the names are
  - sandeep-sandy
  - sandeep-chikkala
- Enable the versioning, ACL enabled, Block all public access

Step - 2:

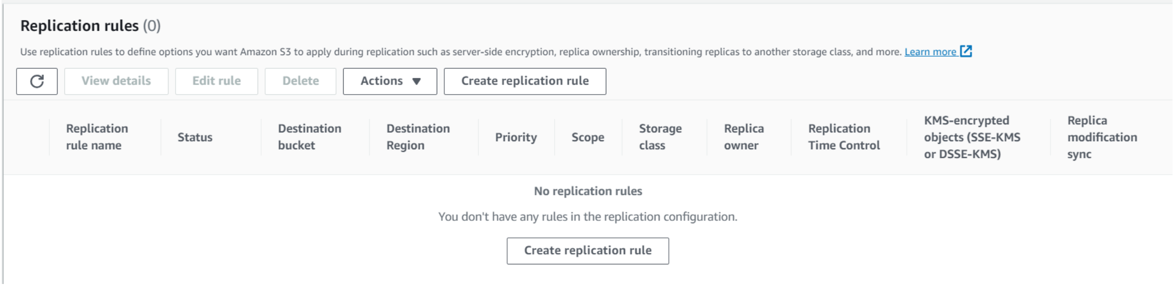
- Here, we have to enable the versioning for 2 buckets

- Go to 1st bucket → management → replication rule → create replication rule → replication name → status - enabled → Click on apply all objects in the bucket → give the destination bucket name



Amazon S3 > Buckets > sandeep-chikkala

sandeep-chikkala



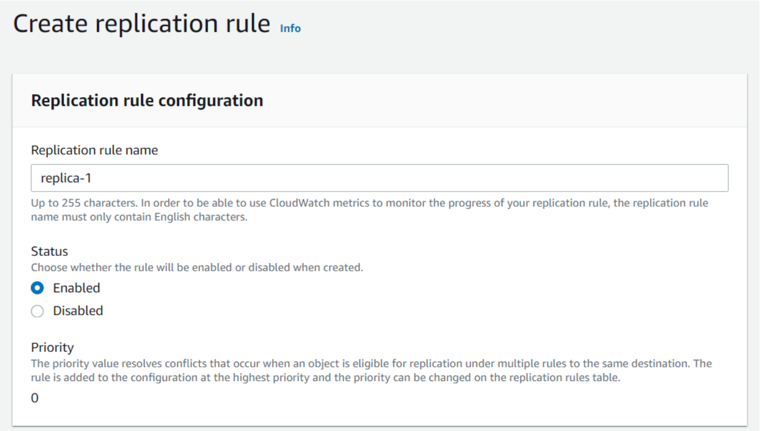
Replication rules (0)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. Learn more

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync

No replication rules

You don't have any rules in the replication configuration.



Create replication rule Info

Replication rule configuration

Replication rule name

replica-1

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status

Choose whether the rule will be enabled or disabled when created.

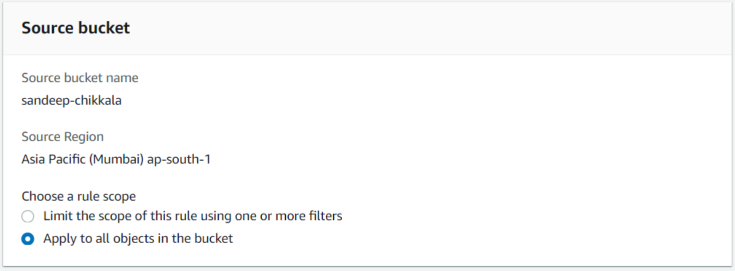
● Enabled

○ Disabled

Priority

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

0



Source bucket

Source bucket name

sandeep-chikkala

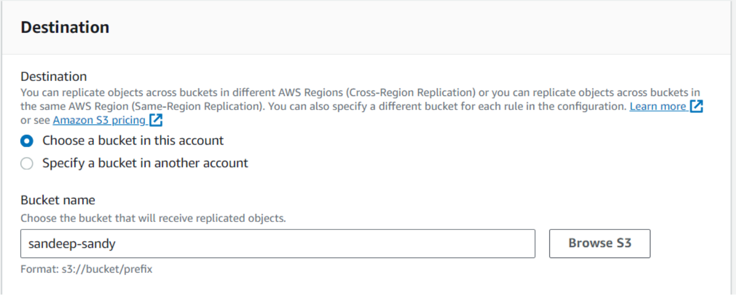
Source Region

Asia Pacific (Mumbai) ap-south-1

Choose a rule scope

○ Limit the scope of this rule using one or more filters

● Apply to all objects in the bucket



Destination

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. Learn more or see Amazon S3 pricing

● Choose a bucket in this account

○ Specify a bucket in another account

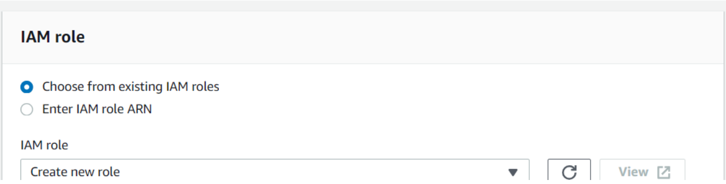
Bucket name

Choose the bucket that will receive replicated objects.

sandeep-sandy

Format: s3://bucket/prefix

In IAM role →choose form existing IAM roles → select Create new role and save



IAM role

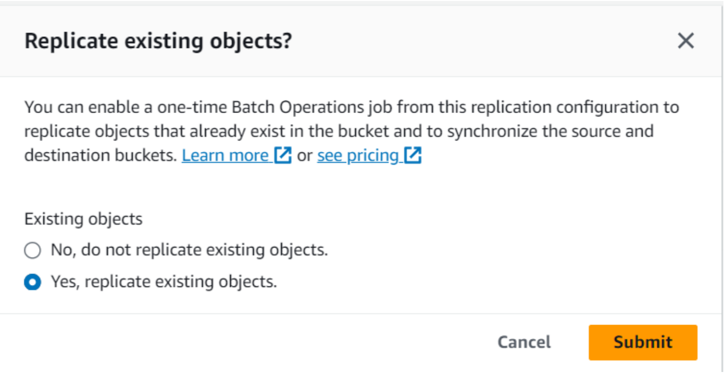
● Choose from existing IAM roles

○ Enter IAM role ARN

IAM role

Create new role ▼

After perform above steps, click on save, it will ask yes (or) no, select yes



Replicate existing objects? ✕

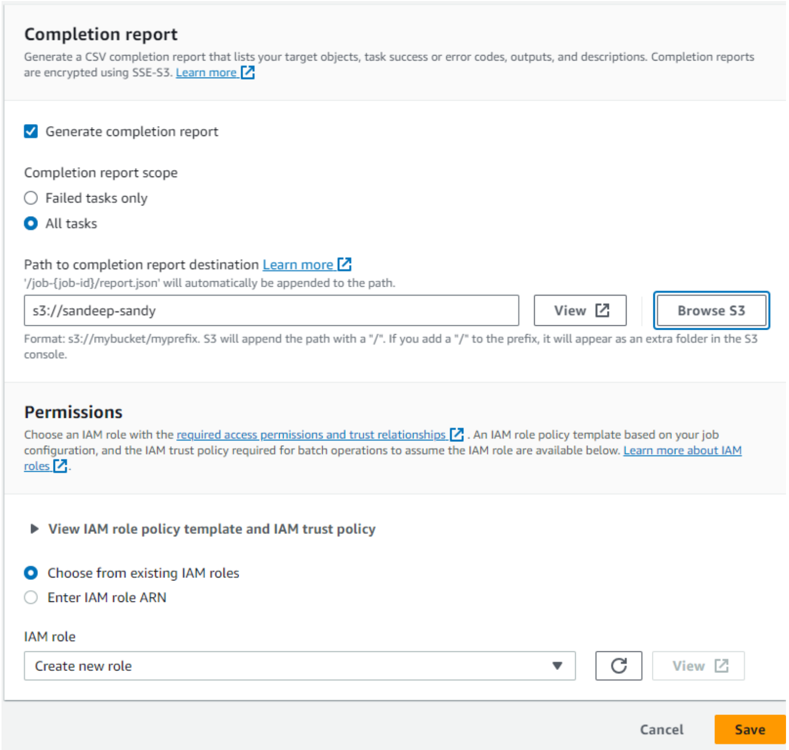
You can enable a one-time Batch Operations job from this replication configuration to replicate objects that already exist in the bucket and to synchronize the source and destination buckets. Learn more or see pricing

Existing objects

○ No, do not replicate existing objects.

● Yes, replicate existing objects.

In the completion report, give bucket-2. For that click on browse S3, select the bucket and click on save



Completion report

Generate a CSV completion report that lists your target objects, task success or error codes, outputs, and descriptions. Completion reports are encrypted using SSE-S3. Learn more

☑ Generate completion report

Completion report scope

○ Failed tasks only

● All tasks

Path to completion report destination Learn more

'/job-{job-id}/report.json' will automatically be appended to the path.

s3://sandeep-sandy

Format: s3://mybucket/myprefix. S3 will append the path with a "/". If you add a "/" to the prefix, it will appear as an extra folder in the S3 console.

Permissions

Choose an IAM role with the required access permissions and trust relationships. An IAM role policy template based on your job configuration, and the IAM trust policy required for batch operations to assume the IAM role are available below. Learn more about IAM roles.

▶ View IAM role policy template and IAM trust policy

● Choose from existing IAM roles

○ Enter IAM role ARN

IAM role

Create new role

Step - 3 :

- So, whatever the step-2, we did for 1st bucket, now we have to do it 2nd bucket. Same like step-2
- So, if you upload a file, based on the size it will takes the time i.e. late replicas
- So, this CRR is worked in different accounts/different regions (or) same regions

Step - 4 :

Now, upload a file in 2nd bucket and check in 1st bucket and enable the show version. You will get the files

Here, overall we can upload the multiple files. But for deleting, it won't replicate. i.e. if you delete a file in bucket-1 the changes didn't reflect in bucket-2

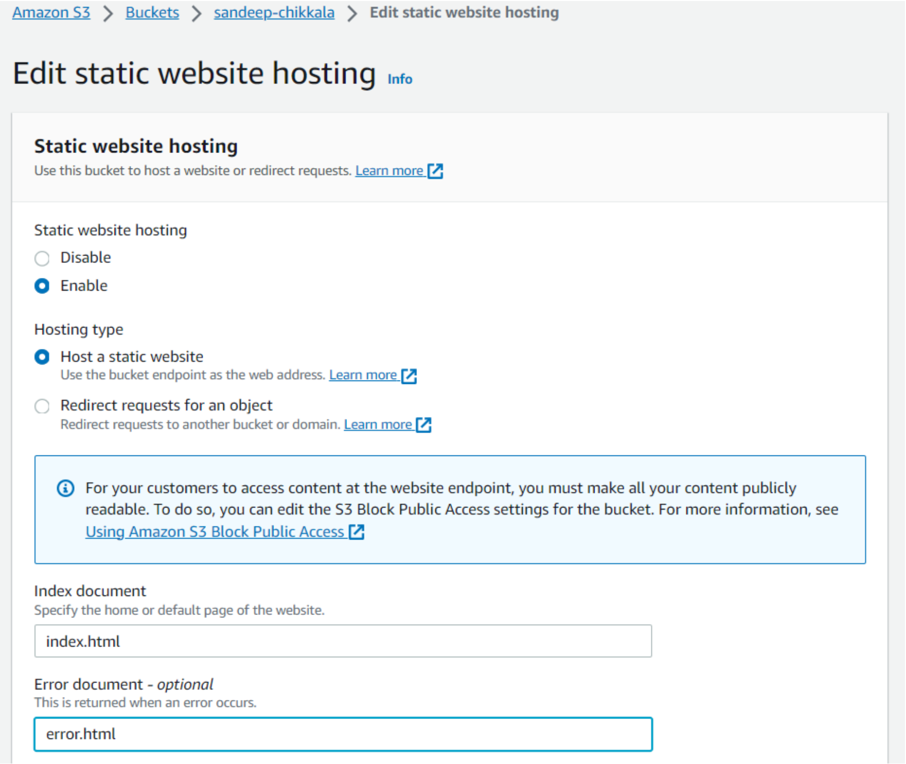
HOSTING THE STATIC WEBSITE MANUALLY IN S3

Websites are two types

- Static Websites
- Dynamic Websites

For hosting the Static websites we're using S3

- First, we need code
- Create a bucket, same like above one → go to properties → click on static website → edit



Amazon S3 > Buckets > sandeep-chikkala > Edit static website hosting

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

○ Disable

● Enable

Hosting type

● Host a static website
Use the bucket endpoint as the web address. Learn more

○ Redirect requests for an object
Redirect requests to another bucket or domain. Learn more

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Index document
Specify the home or default page of the website.

index.html

Error document - *optional*
This is returned when an error occurs.

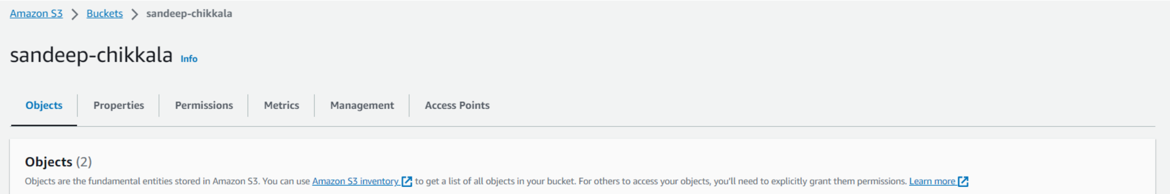
error.html

  - So, here for any website we are having home page. i.e. index.html
  - If the site is in under maintenance. So, that issue users want to know means that time they have to visible like a page called "error.html"
- After perform above data, click on save changes

So, first create 2 files in local with the same names

- index.html → <html><h1> hi this is static website </h1></html> → creating html page
- error.html → <html><h1> error </h1></html> → creating error page

Now, upload this 2 files in the bucket

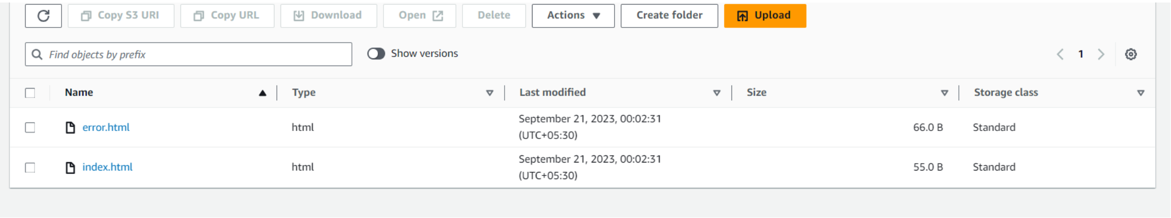


Amazon S3 > Buckets > sandeep-chikkala

sandeep-chikkala Info

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more



□	Name ▲	Type	Last modified	Size	Storage class
□	error.html	html	September 21, 2023, 00:02:31 (UTC+05:30)	66.0 B	Standard
□	index.html	html	September 21, 2023, 00:02:31 (UTC+05:30)	55.0 B	Standard

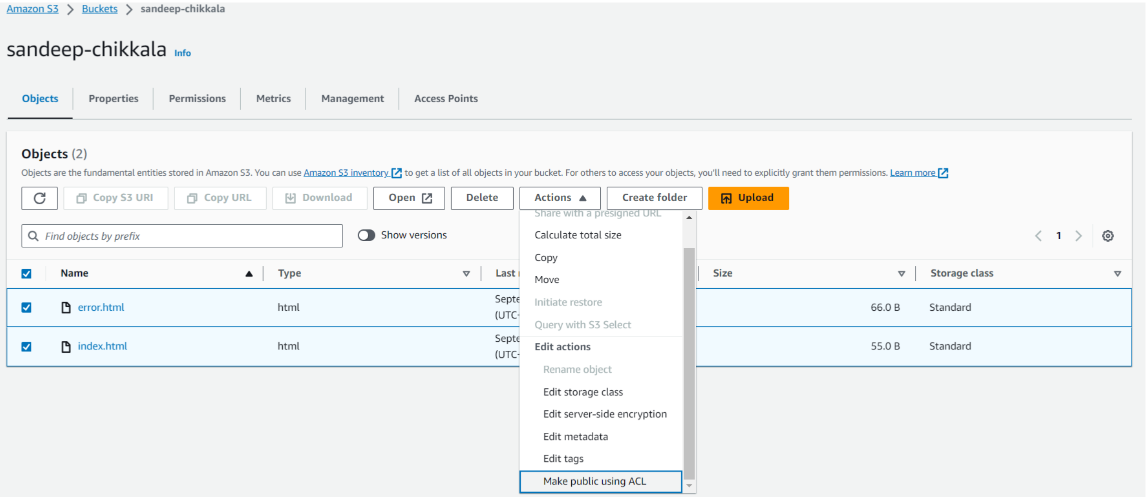
- So, when you select the object and copy the URL in browser, you will get output

(or)

- Go to properties → static hosting → and from we can copy the URL and paste in browser
- But, here we are getting permission denied errors.

For that, we have to do two things

1. Select the files inside objects and click on actions → select option "make public using ACL"


Amazon S3 > Buckets > sandeep-chikkala

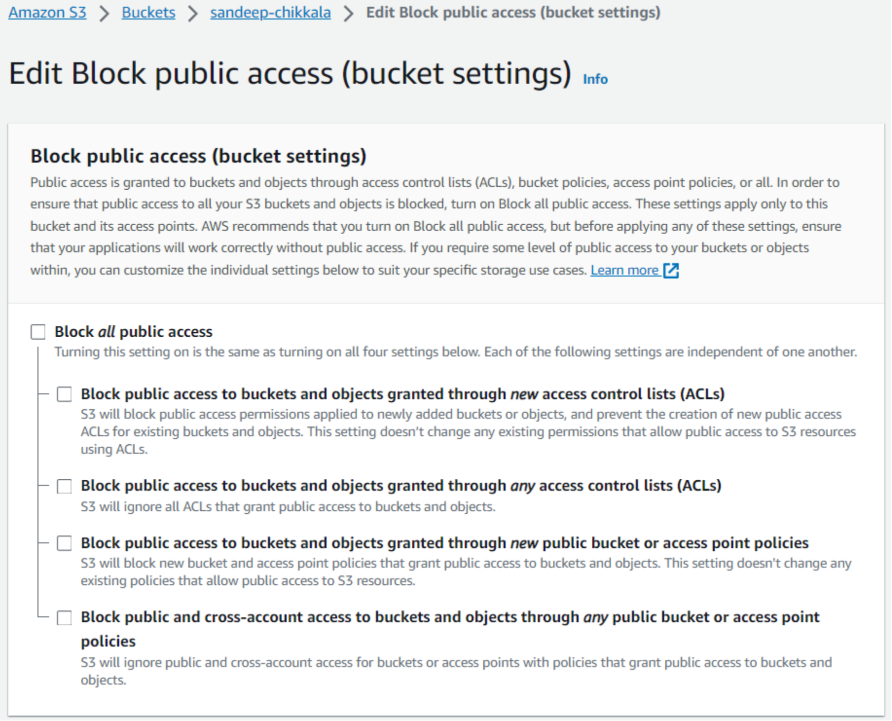
sandeep-chikkala Info

Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name ▲	Type	Last	Size	Storage class
☑	error.html	html	Septe (UTC-	66.0 B	Standard
☑	index.html	html	Septe (UTC-	55.0 B	Standard

2. Go to Permissions → select block public access → edit


Amazon S3 > Buckets > sandeep-chikkala > Edit Block public access (bucket settings)

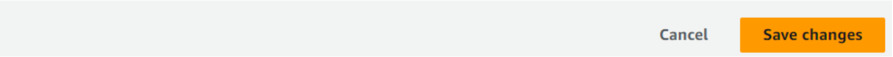
Edit Block public access (bucket settings) Info

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

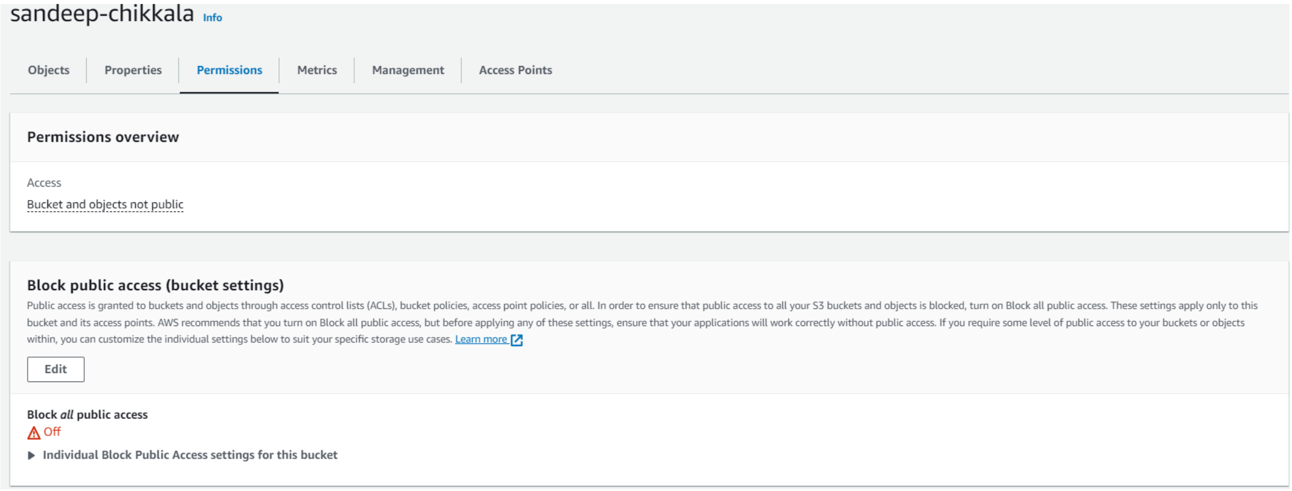
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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.



Here, uncheck everything and click on save changes

After doing changes, we will get like below image



Permissions overview

Access
Bucket and objects not public

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
⚠ Off

▶ Individual Block Public Access settings for this bucket

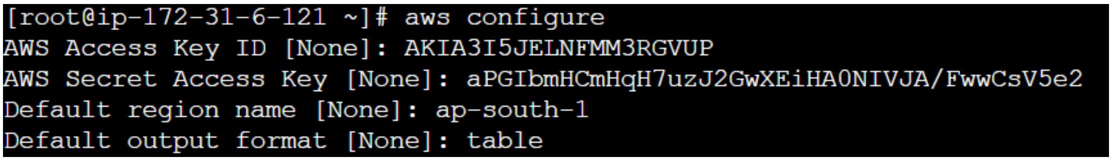
So, now you can access the static websites in browser to see the output

S3 - CLI

Through CLI, w can create, delete the buckets (or) objects

CLI Syntax : cloud service command

1. See list of buckets
    - aws s3 ls
2. Run - aws configure
    - Here, you have to provide access key and secret key
    - For that using IAM we have to create
    - Go to user → create user → After creation is completed → click on user → click on security credentials → click on access key → select CLI (or) third party service → create
    - Enter the details like this in the given below



```
[root@ip-172-31-6-121 ~]# aws configure
AWS Access Key ID [None]: AKIA3I5JELNFMM3RGVUP
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: table
```

1. Create a bucket
    - aws s3 mb s3://Bucketname
    - Here, mb → make bucket
    - Now, perform, aws s3 ls → you are having buckets
2. Delete the bucket
    - aws s3 rb s3://Bucketname
    - Here, rb → remove bucket
3. See the list of files/objects inside the bucket
    - aws s3 ls s3://Bucketname

4. Send a file from server to S3
    - touch aws.jpg
        - aws s3 cp aws.jpg s3://Bucketname
    - Check in S3, you will have the data
5. Download the bucket inside file in server
    - Go to S3 → select file → Copy S3 URI
        - aws s3 cp "S3URI" .
    - ll → you are having bucket files in your server
6. Delete the objects inside the bucket
    - aws s3 rm s3://Bucketname --recursive
    - Check in s3
7. Delete the bucket & file at a time
    - aws s3 rb s3://Bucketname --force
    - file deleted
    - Bucket deleted

Sync : It is a command used to send a files from one bucket to another bucket