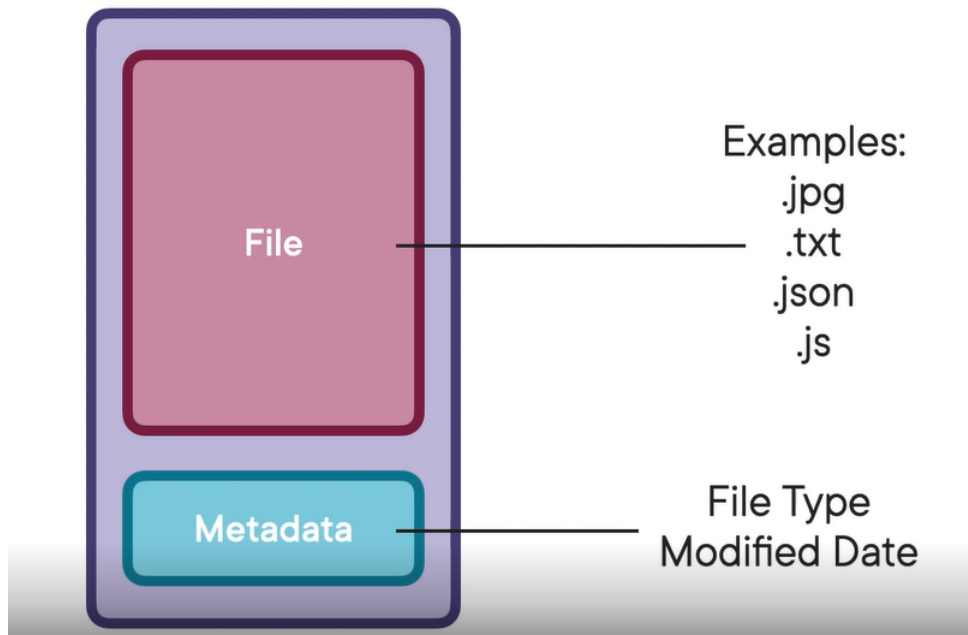


Hosting all the things with S3:

S3 overview:

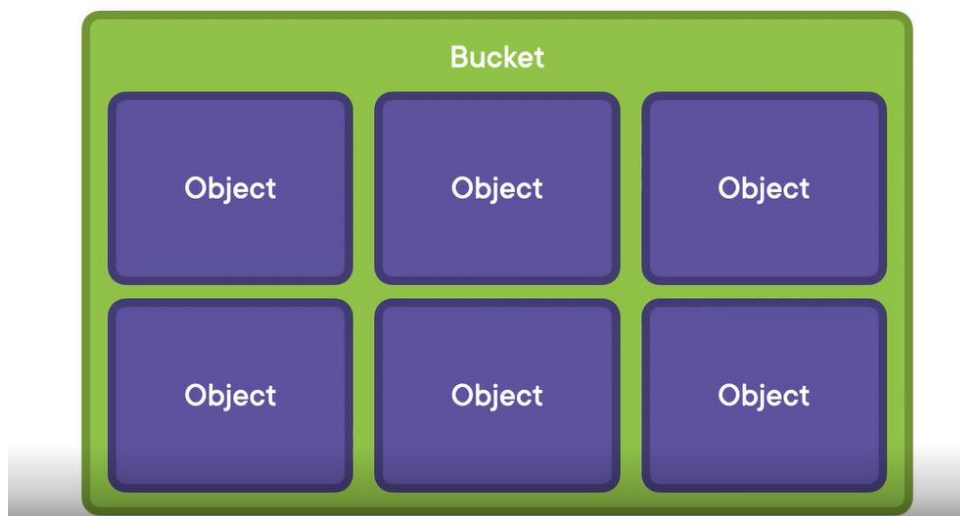
- Simple storage service
- AWS service for storing files

S3 Object



- The maximum object size in S3 is 5 TB.

S3 Bucket



S3 object key example:

File Name: image.png

Folder Name: images

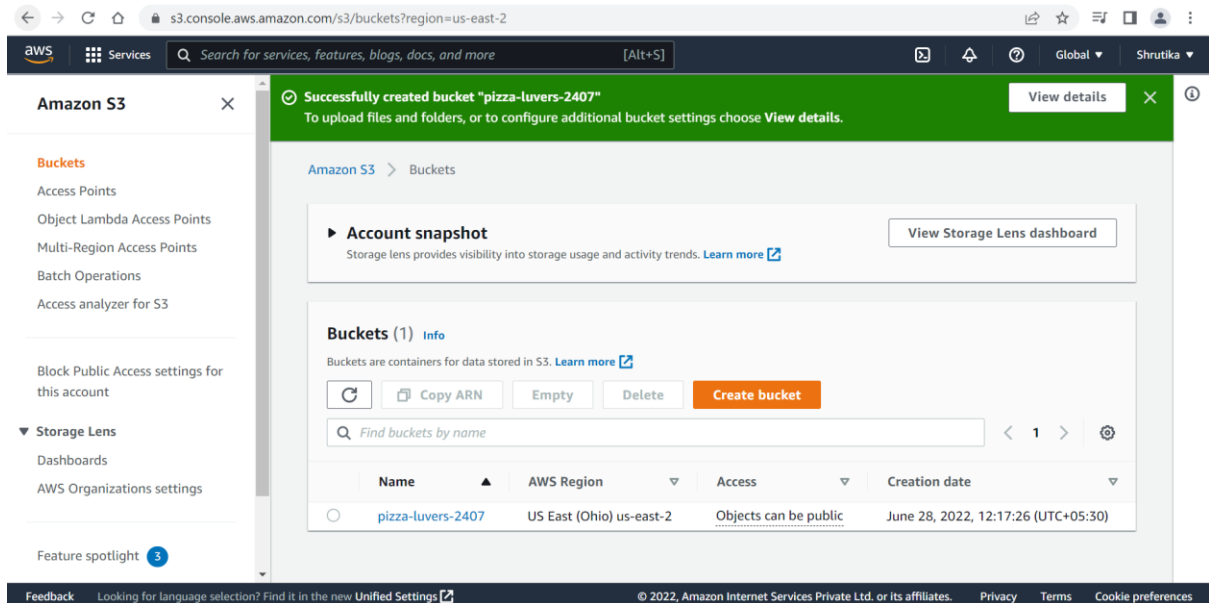
Object Key: images/image.png

- CloudFront is the best way to solve geographic latency.

Creating an S3 bucket:

The screenshot shows the 'Create bucket' page in the AWS S3 console. The browser address bar shows the URL: `s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2`. The page has a blue header with the AWS logo and a search bar. Below the header, a blue banner contains a message about S3 console improvements and a 'Provide feedback' button. The main content area is titled 'Create bucket' with an 'Info' link. Below this, it says 'Buckets are containers for data stored in S3. [Learn more](#)'. The 'General configuration' section contains a 'Bucket name' input field with the text 'pizza-luvers-2407', an 'AWS Region' dropdown menu set to 'US East (Ohio) us-east-2', and a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. The footer of the console shows a 'Feedback' link, a language selection prompt, and copyright information for 2022.

The screenshot shows the 'Block Public Access settings for this bucket' page in the AWS S3 console. The browser address bar shows the URL: `s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2`. The page has a blue header with the AWS logo and a search bar. Below the header, a blue banner contains a message about S3 console improvements and a 'Provide feedback' button. The main content area is titled 'Block Public Access settings for this bucket'. It contains a paragraph explaining that public access is granted through ACLs, bucket policies, access point policies, or all, and that turning on 'Block all public access' will block public access to the bucket and its objects. Below this, there are four checkboxes, all of which are unchecked:
1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
At the bottom of the settings section, there is a warning icon and text: 'Turning off block all public access might result in this bucket and the objects within becoming public'. The footer of the console shows a 'Feedback' link, a language selection prompt, and copyright information for 2022.



Uploading objects to S3:

How to Upload Objects to S3

Console

Adhoc or
Small Number
of File Uploading

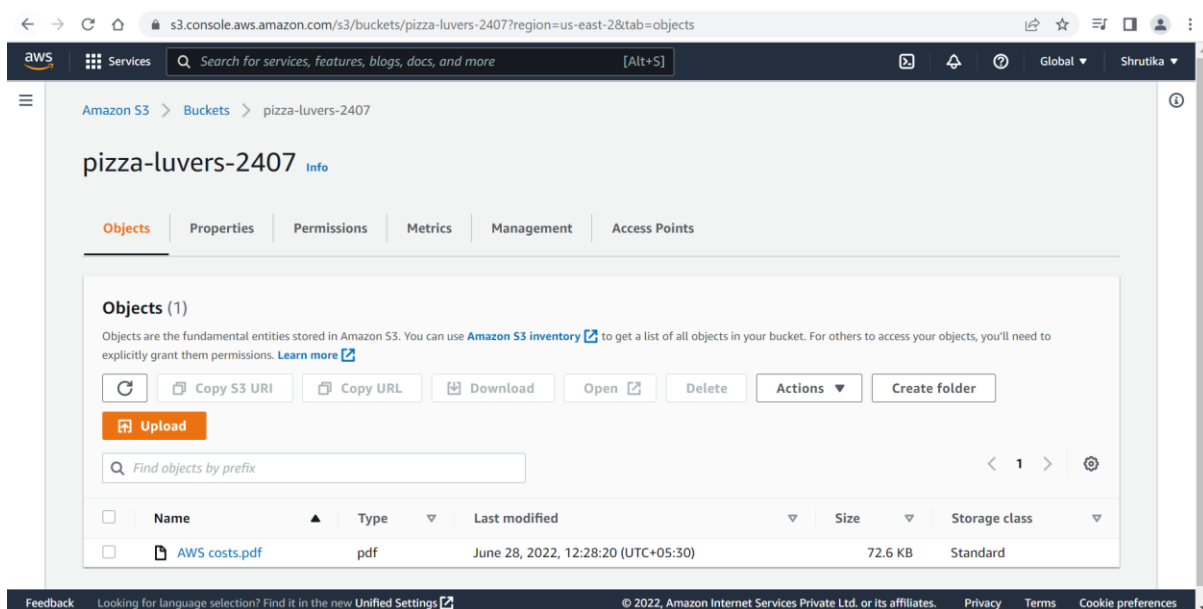
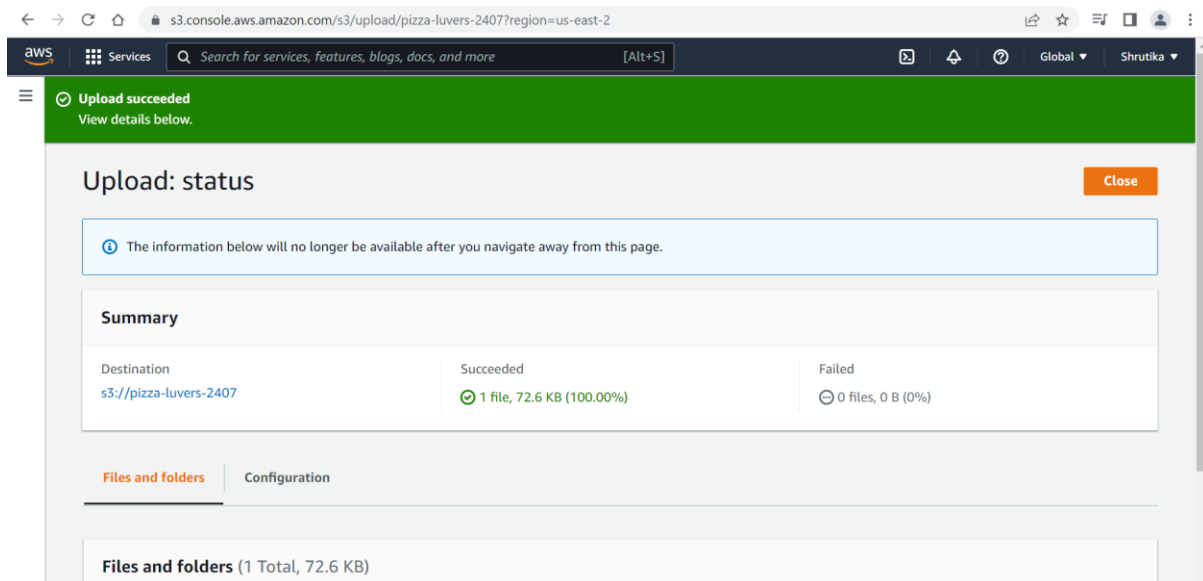
CLI

Recursive
Directory
Uploading

SDK

Dynamic
in Code
Uploading

The AWS CLI has the permissions given to the user whose key is configured on your system.



- Amazon S3 is an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects.
- To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region. Then, you upload your data to that bucket as objects in Amazon S3. Each object has a key (or key name), which is the unique identifier for the object within the bucket.
- S3 provides features that you can configure to support your specific use case. For example, you can use S3 Versioning to keep multiple versions of an object in the same bucket, which allows you to restore objects that are accidentally deleted or overwritten.

- Buckets and the objects in them are private and can be accessed only if you explicitly grant access permissions. You can use bucket policies, AWS Identity and Access Management (IAM) policies, access control lists (ACLs), and S3 Access Points to manage access.