Simple Storage Service (S3)

Object-based storage service.
Serverless storage in the cloud.
Don't worry about filesystems or disk space.

Introduction to S3

What is Object Storage (Object-based Storage)?

data storage architecture that manages data as objects, **as opposed** to other storage architectures:

- **file systems** which manages data as a files and fire hierarchy, and
- **block storage** which manages data as blocks within sectors and tracks.

S3 provides you with **unlimited storage**. You don't need to think about the underlying infrastructure

The S3 Console provides an interface for you to upload and access your data

S3 Object

Objects contain your data. They are like files.
Object may consist of:

- **Key** this is the name of the object
- **Value** the data itself made up of a sequence of bytes
- **Version ID** when versioning enabled, the version of object
- **Metadata** additional information attached to the object

You can store data from **0 Bytes** to **5 Terabytes** in size

S3 Bucket

Buckets hold objects. Buckets can also have folders which in turn hold objects

S3 is a universal namespace so bucket names must be unique (think like having a domain name)

S3 – Storage Classes

Trade **Retrieval Time, Accessibility and Durability** for **Cheaper Storage**

11 9's (Eleven Nines) = 99.99999999999%
9 9's (Nine Nines) = 99.999999999%

Cheaper it gets

Standard (default)	Fast! 99.99% Availability, **11 9's** Durability. Replicated across at least three AZs
Intelligent Tiering*	Uses ML to analyze your object usage and determine the appropriate storage class. Data is moved to the most cost-effective access tier, without any performance impact or added overhead.
Standard Infrequently Accessed (IA)	Still Fast! Cheaper if you access files less than once a month. Additional retrieval fee is applied. **50% less** than Standard (reduced availability)
One Zone IA	Still Fast! Objects only exist in one AZ. Availability (is 99.5%). but cheaper than Standard IA by 20% less (Reduce durability) Data could get destroyed. A retrieval fee is applied.
Glacier	For long-term cold storage. Retrieval of data can take minutes to hours but the off is very cheap storage
Glacier Deep Archive	The lowest cost storage class. Data retrieval time is 12 hours.

S3 – Storage Classes Comparison

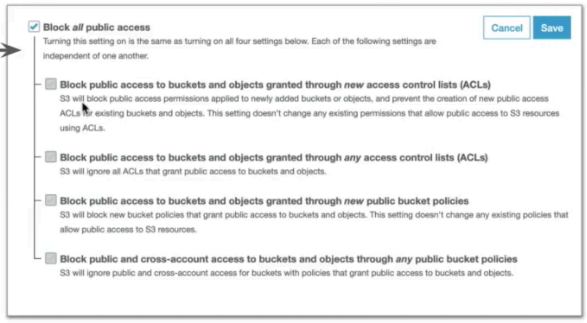
	Standard	Intelligent Tiering	Standard IA	One-Zone IA	Glacier	Glacier Deep Archive
Durability	11 9's	11 9's	11 9's	11 9's	11 9's	11 9's
Availability	99.99%	99.9%	99.9%	99.5%	N/A	N/A
Availability SLA	99.99%	99%	99%	99%	N/A	N/A
AZs	>3	>3	>3	1	>3	>3
Min Capacity charge per object	N/A	N/A	128kb	128kb	40kb	40kb
Min storage duration charge	N/A	30 days	30 days	30 days	90 days	180 days
Retrieval fee	N/A	N/A	Per GB	Per GB	Per GB	Per GB
First byte latency	ms	ms	ms	ms	mins to hours	hours

S3 Guarantees

Platform is built for 99.99% availability
Amazon guarantee 99.9% availability
Amazon guarantees 11' 9s of durability

S3 - Security

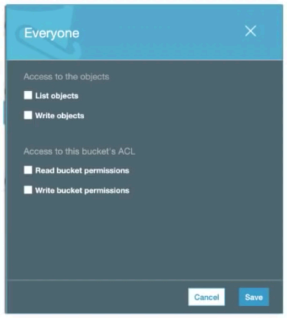
All new buckets are **PRIVATE** when created by default



Logging per request can be turned on a bucket
Log files are generated and saved in a different bucket.
(even a bucket in a different AWS account if desired)

Access control is configured using **Bucket Policies** and **Access Control Lists (ACL)**

Access Control Lists



Legacy feature (but not deprecated) of controlling access to buckets and objects.

Simple way of granting access

Bucket Policies

Use a policy to define complex rule access.

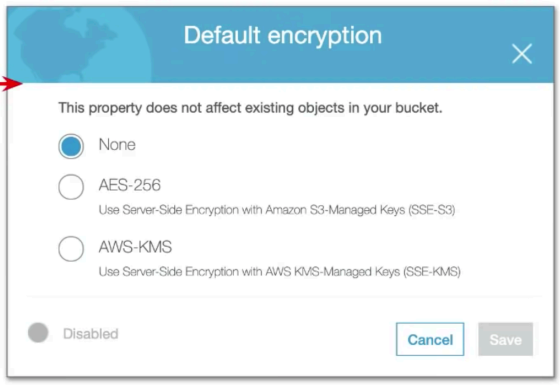
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::www.exampro.co/*"
        }
    ]
}
```

S3 – Encryption

Encryption In Transit
Traffic between your local host and S3 is achieved via **SSL/TLS**

Server Side Encryption (SSE) - Encryption At Rest
Amazon help you encrypt the object data
S3 Managed Keys - (Amazon manages all the keys)
SSE-AES S3 handles the key, uses AES-256 algorithm
SSE-KMS Envelope encryption, AWS KMS and you manage the keys
SSE-C Customer provided key (you manage the keys)

Client-Side Encryption
You encrypt your own files before uploading them to S3



S3 – Data Consistency

New Objects (PUTS)

Read After Write Consistency

When you upload a new S3 object you are able **read immediately** after writing.

Overwrite (PUTS) or Delete Objects (DELETES)

Eventual Consistency

When you overwrite or delete an object it takes time for S3 to replicate versions to AZs.

If you were to read immediately, S3 may return you an old copy. You need to generally wait a few seconds before reading.

S3 – Data Consistency

New Objects (PUTS)

Read After Write Consistency

When you upload a new S3 object you are able **read immediately** after writing.

Overwrite (PUTS) or Delete Objects (DELETES)

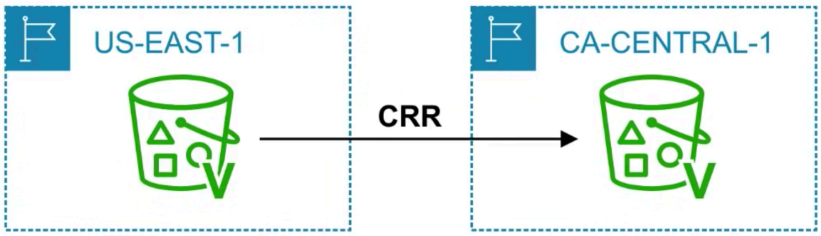
Eventual Consistency

When you overwrite or delete an object it takes time for S3 to replicate versions to AZs.

If you were to read immediately, S3 may return you an old copy. You need to generally wait a few seconds before reading.

S3 – Cross Region Replication (CRR)

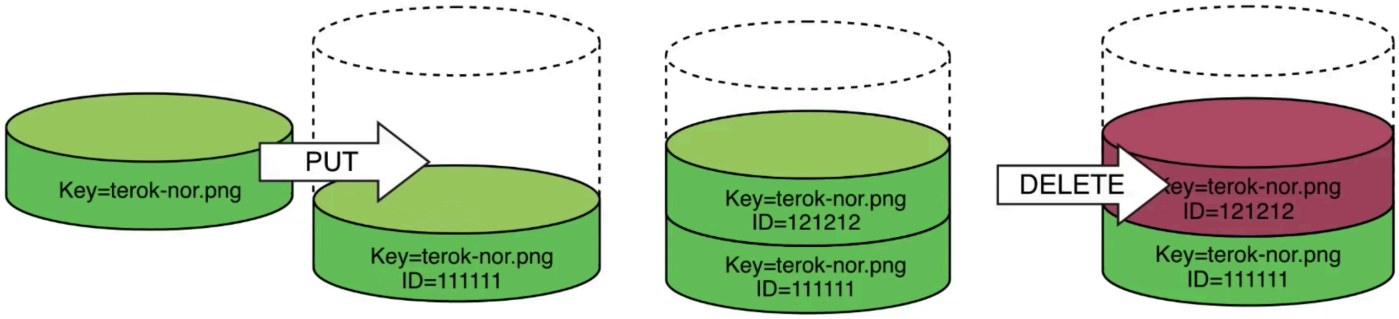
When enabled, any object that is uploaded will be **automatically replicated** to another region(s)
Provides higher durability and potential disaster recovery for objects



You must have **versioning** turned on both the **source** and **destination** buckets.
You can have CRR replicate to another AWS account

S3 Versioning

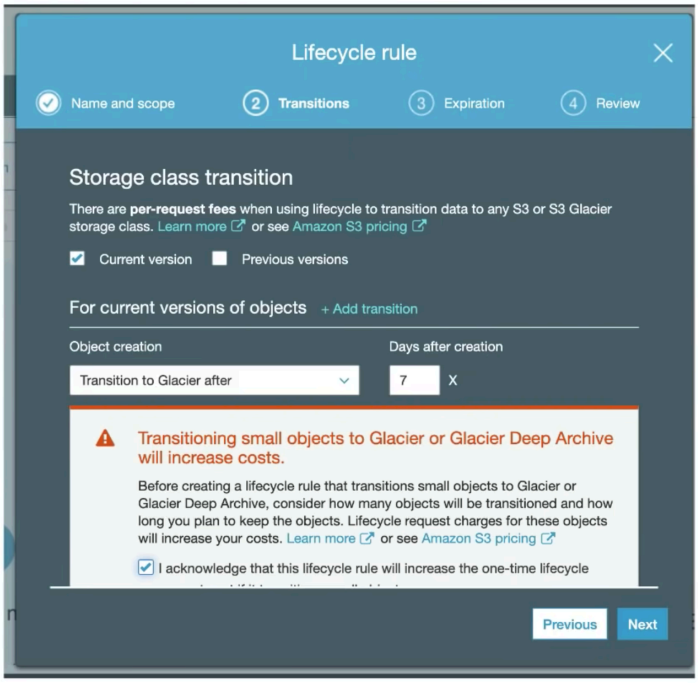
- Store all versions of an object in S3
- Once enabled it cannot be disabled, only suspended on the bucket
- Fully integrates with S3 Lifecycle rules
- MFA Delete feature provides extra protection against deletion of your data



S3 Lifecycle Management

Automate the process of moving objects to different Storage classes or deleting objects all together.

Can be used together with **versioning**
Can be applied to both **current** and **previous** versions



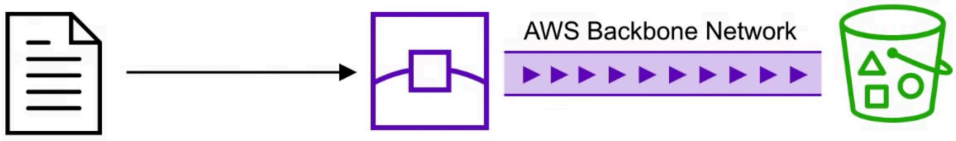
S3 – Transfer Acceleration

Fast and secure transfer of files **over long distances** between your end users and an S3 bucket.

Utilizes **CloudFront's** distributed **Edge Locations.**

Instead of uploading to your bucket, users use a **distinct URL** for an Edge Location

As data arrives at the Edge Location it is automatically routed to S3 over a specially optimized network path. (Amazon's backbone network)



S3 – Presigned Urls

Generate a url which provides you temporary access to an object to either upload or download object data. Presigned Urls are commonly used **to provide access to private objects**. You can use AWS CLI or AWS SDK to generate Presigned Urls.

```
aws s3 presign s3://mybucket/myobject  --expires-in 300
```

```
https://mybucket.s3.amazonaws.com/myobject?AWSAccessKeyId=AKIAJXXXXXXXXXXXXXX&Expires=1503602631&Signature=ibOGfAovnhIF13DALdAgsdtg2s%3D
```

You have a web-application which needs to allow users to download files from a password protected part of your web-app. Your web-app generates presigned url which expires after 5 seconds. The user downloads the file.

S3 - MFA Delete

MFA Delete ensures users cannot delete objects from a bucket unless they provide their MFA code.

MFA Delete can only be enabled under these conditions

1. The **AWS CLI** must be used to turn on MFA
2. The bucket must have **versioning turned on**


```
aws s3api put-bucket-versioning \
    --bucket bucketname \
    --versioning-configuration Status=Enabled,MFADelete=Enabled \
    --mfa "your-mfa-serial-number mfa-code" \
```

Only the bucket owner logged in as Root User can DELETE objects from bucket

S3 CheatSheet

- **Simple Storage Service** (S3) Object-based storage. Store **unlimited** amount of data without worry of underlying storage infrastructure
- S3 replicates data across at least 3 AZs to ensure 99.99% Availability and 11' 9s of durability
- Objects contain your data (they're like files)
- Objects can be size anywhere from **0 Bytes** up to 5 Terabytes
- Buckets contain objects. Buckets can also contain folders which can in turn can contain objects.
- Bucket names are unique across all AWS accounts. Like a domain name.
- When you upload a file to S3 successfully you'll receive a HTTP 200 code
  Lifecycle Management Objects can be moved between storage classes or objects can be deleted automatically based on a schedule
- **Versioning** Objects are giving a Version ID. When new objects are uploaded the old objects are kept. You can access any object version. When you delete an object the previous object is restored. Once Versioning is turned on it cannot be turn off, only suspended.
- **MFA Delete** enforce DELETE operations to require MFA token in order to delete an object. Must have versioning turned on to use. Can only turn on MFA Delete from the AWS CLI. Root Account is only allowed to delete objects
- All new buckets are **private by default**
- Logging can be turned to on a bucket to log to track operations performed on objects
- **Access control** is configured using **Bucket Policies** and **Access Control Lists (ACL)**
- **Bucket Policies** are JSON documents which let you write complex control access
- **ACLs** are the legacy method (not deprecated) where you grant access to objects and buckets with simple actions

S3 CheatSheet

- **Security in Transit** Uploading files is done over SSL
- **SSE** stands for Server Side Encryption. S3 has **3 options** for SSE.
- **SSE-AES** S3 handles the key, uses AES-256 algorithm
- **SSE-KMS** Envelope encryption via AWS KMS and you manage the keys
- **SSE-C** Customer provided key (you manage the keys)
- **Client-Side Encryption** You must encrypt your own files before uploading them to S3
- **Cross Region Replication (CRR)** allows you to replicate files across regions for greater durability. You must have versioning turned on in the source and destination bucket. You can have CRR replicate to bucket in another AWS Account
- **Transfer Acceleration** provide faster and secure uploads from anywhere in the world. data is uploaded via distinct url to an Edge Location. Data is then transported to your S3 bucket via AWS backbone network.
- **Presigned Urls** is a url generated via the AWS CLI and SDK. It provides temporary access to write or download object data. Presigned Urls are commonly used to access private objects.

S3 CheatSheet

- S3 has **6 different** Storage Classes:
  - **Standard** Fast! 99.99% Availability, 11 9's Durability. Replicated across at least three AZs
  - **Intelligent Tiering** Uses ML to analyze your object usage and determine the appropriate storage class. Data is moved to the most cost-effective access tier, without any performance impact or added overhead.
  - **Standard Infrequently Accessed (IA)** Still Fast! Cheaper if you access files less than once a month. Additional retrieval fee is applied. 50% less than Standard (reduced availability)
  - **One Zone IA** Still Fast! Objects only exist in one AZ. Availability (is 99.5%). but cheaper than Standard IA by 20% less (Reduce durability) Data could get destroyed. A retrieval fee is applied.
  - **Glacier** For long-term cold storage. Retrieval of data can take minutes to hours but the off is very cheap storage
  - **Glacier Deep Archive** The lowest cost storage class. Data retrieval time is 12 hours.