

6. S3 Buckets

⌚ Created	@August 31, 2022 12:19 AM
✖ Class	
✖ Type	
✖ Materials	
✓ Reviewed	<input type="checkbox"/>
☰ Property	
📅 Date	

S3 Bucket Policies

Resource Policies

Identity policy

The screenshot shows the AWS S3 Bucket Policies interface. On the left, a JSON policy document is displayed:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::secretcatproject/*"]
    }
  ]
}
```

A purple arrow points from the "Principal": "*" line in the JSON to the "secretcatproject" bucket icon on the right. The bucket icon is a green bucket with a white handle, labeled "secretcatproject". Above the bucket is the AWS logo. Below the bucket is a red arrow pointing towards it. At the bottom of the interface, a text box contains the following note:

So the policy is attached to a bucket in this case.

To differentiate between two policies in the s3. if policy have "Principle" mentioned inside it means that it is most like a resource policy

Bucket Policy: should be default thought when granting access to anonymous.

So much security ... help

• Identity : Controlling different resources

• Identity : You have a preference for IAM

• Identity : **Same account**

• Bucket : Just controlling S3

• Bucket : **Anonymous or Cross-Account**

• ACLs : **NEVER** - unless you must
much of the time is a preference thing.

S3 Static website hosting and demo

Done

Object Versioning and MFA Delete

Disabled by default but once enabled you cannot disable it but you can suspend it and if you want you can enable it from suspended.



Object Versioning

<https://learn.cantrill.io>

adriancantrill

- ...**cannot be switched** off - only suspended
- Space is consumed by ALL versions
- You are billed for ALL versions
- Only way to 0 costs - is to delete the bucket

Now, there's one other

MFA Delete:



MFA Delete

<https://learn.cantrill.io>

adriancantrill

- Enabled in **versioning configuration**
- MFA is required to change bucket **versioning state**
- MFA is required to **delete versions**
- Serial number (MFA) + Code passed with API CALLS

Object Encryption:

====

can be found on ipad notes

S3 encryption:

Buckets itself are not encrypted

objects are the one which are encrypted

encryption is at object level

Client side encryption:

this means that encryption is done at from starting point which is client

so client has to

secure key

manage encryption key

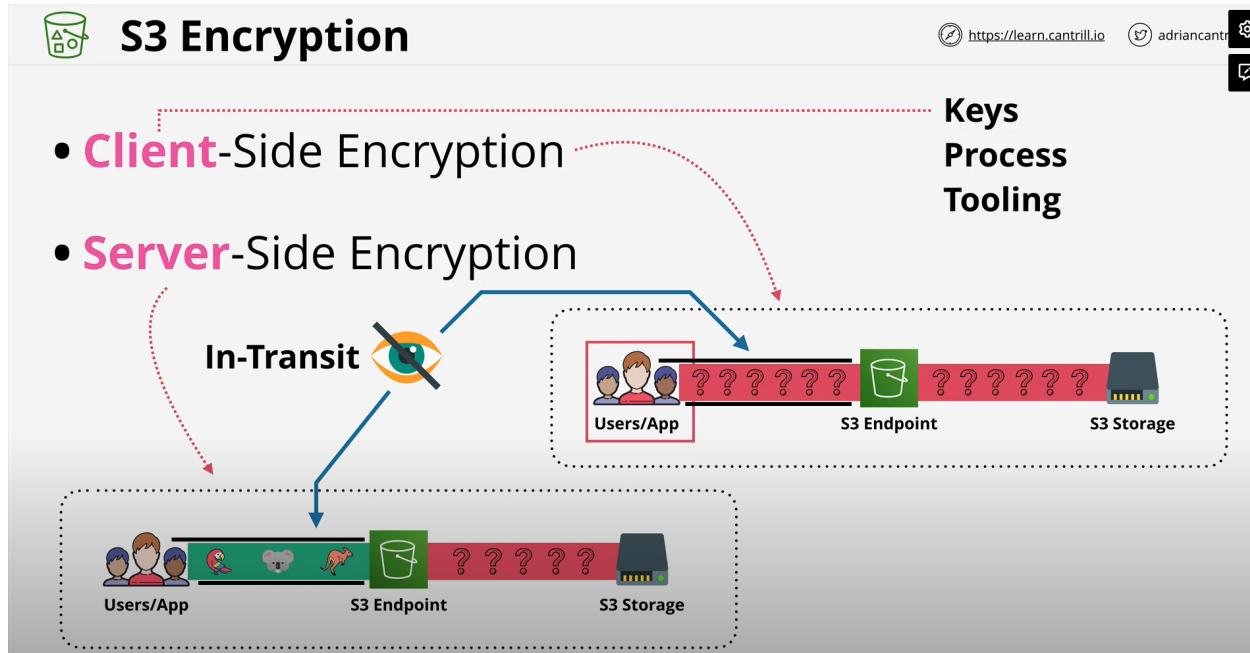
s3 see it as scrambled data

Server Side encryption:

s3 handles encryption

s3 secures the key

this is applied when data from user is at s3 then encryption is applied and it send to s3 storage



Server-Side Encryption type:



S3 Encryption

<https://learn.cantrill.io> adriancantrill

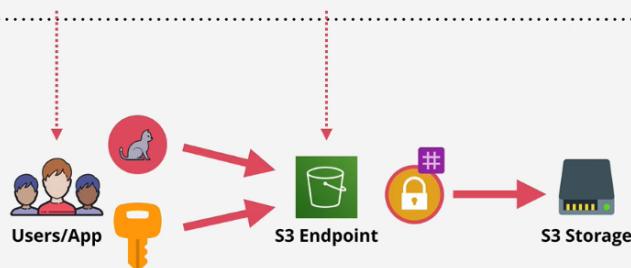
- Server-Side Encryption with Customer-Provided Keys (**SSE-C**)
- Server-Side Encryption with Amazon S3-Managed Keys (**SSE-S3**)
- Server-Side Encryption with Customer Master Keys (CMKs) Stored in AWS Key Management Service (**SSE-KMS**)



SSE-C

<https://learn.cantrill.io> adriancantrill

Manages Keys Manages Encryption

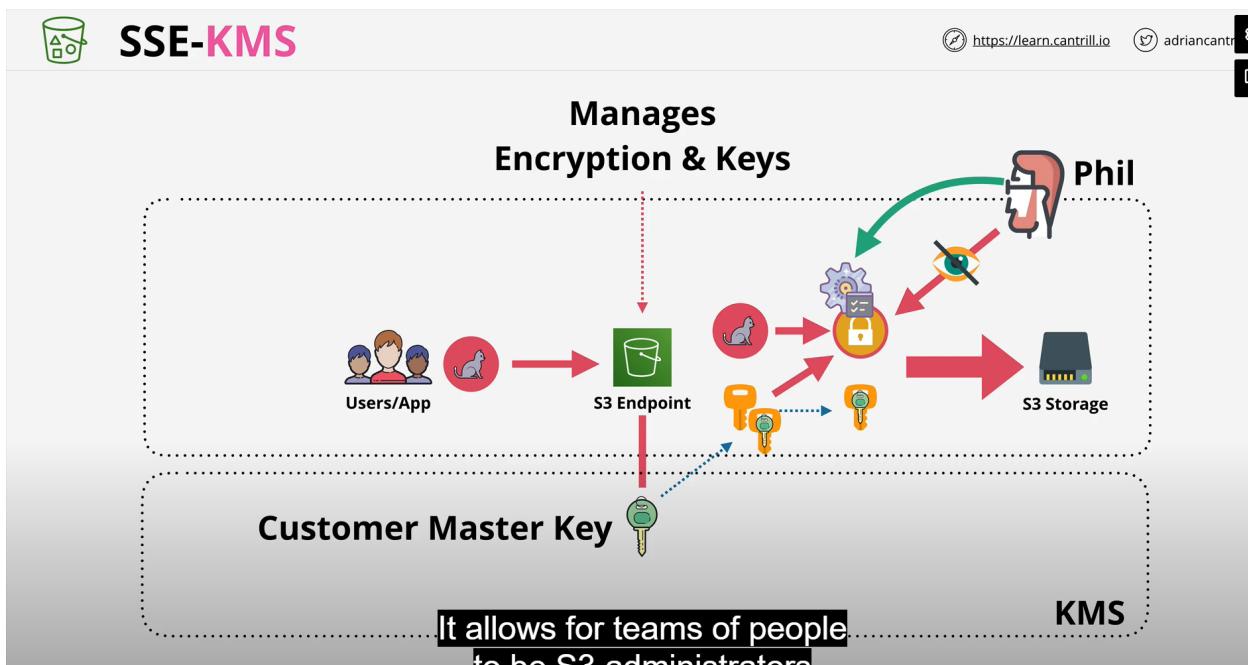
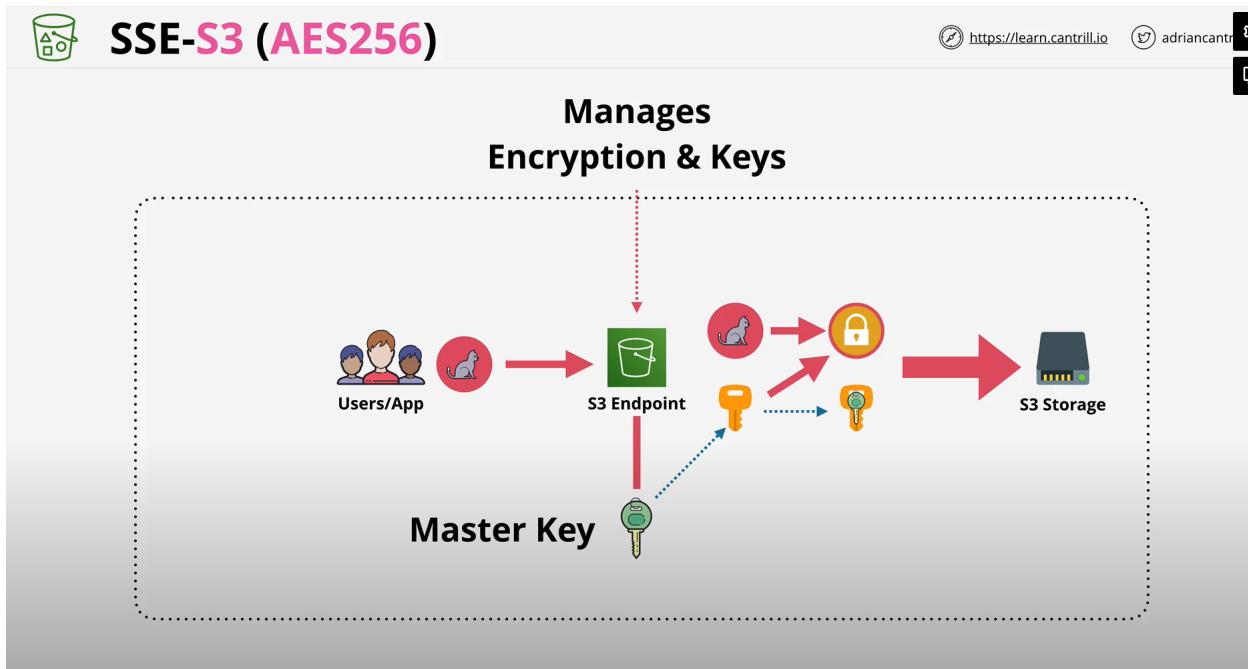


SSE-S3

Not able to control the keys by user

admin don't have much control over key as AWS handles the key

USES AES 256 Encryption algorithm



The screenshot shows a video player interface with a dark theme. At the top, there are controls for subtitles (Off), a search bar containing 'nary', and links to 'https://learn.cantrill.io' and 'adriancantrill'. Below the search bar are icons for settings and sharing. The main content is a table with four columns: Method, Key Management, Encryption Processing, and Extras.

Method	Key Management	Encryption Processing	Extras
Client-Side	YOU	YOU	
SSE-C	YOU	S3	
SSE-S3	S3	S3	
SSE-KMS	S3 & KMS	S3	Rotation Control Role Separation

S3 Storage Classes:

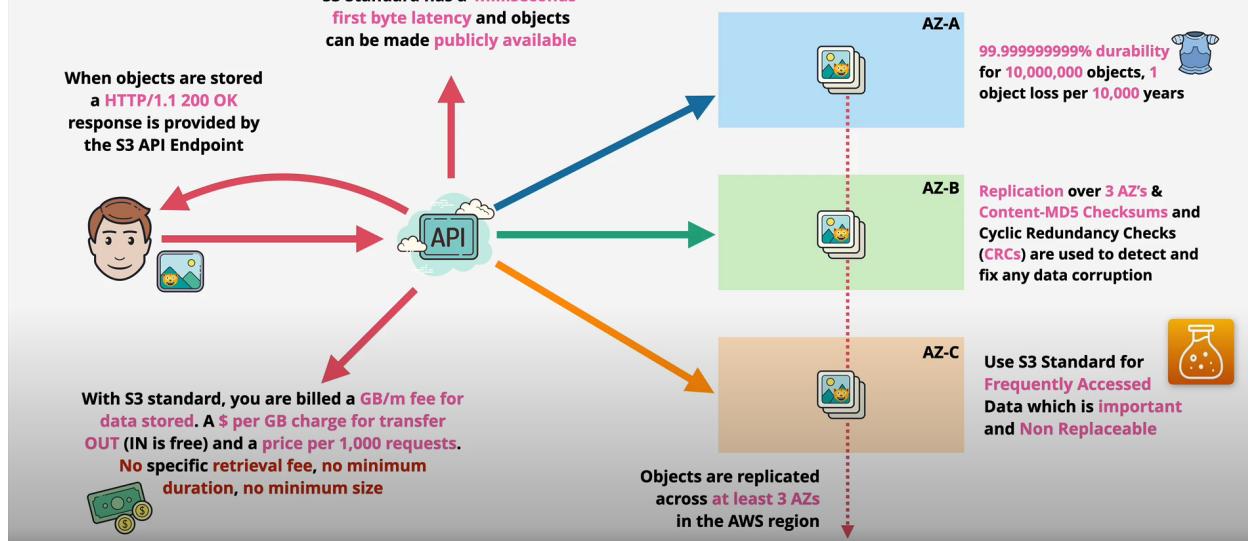
s3 standard:



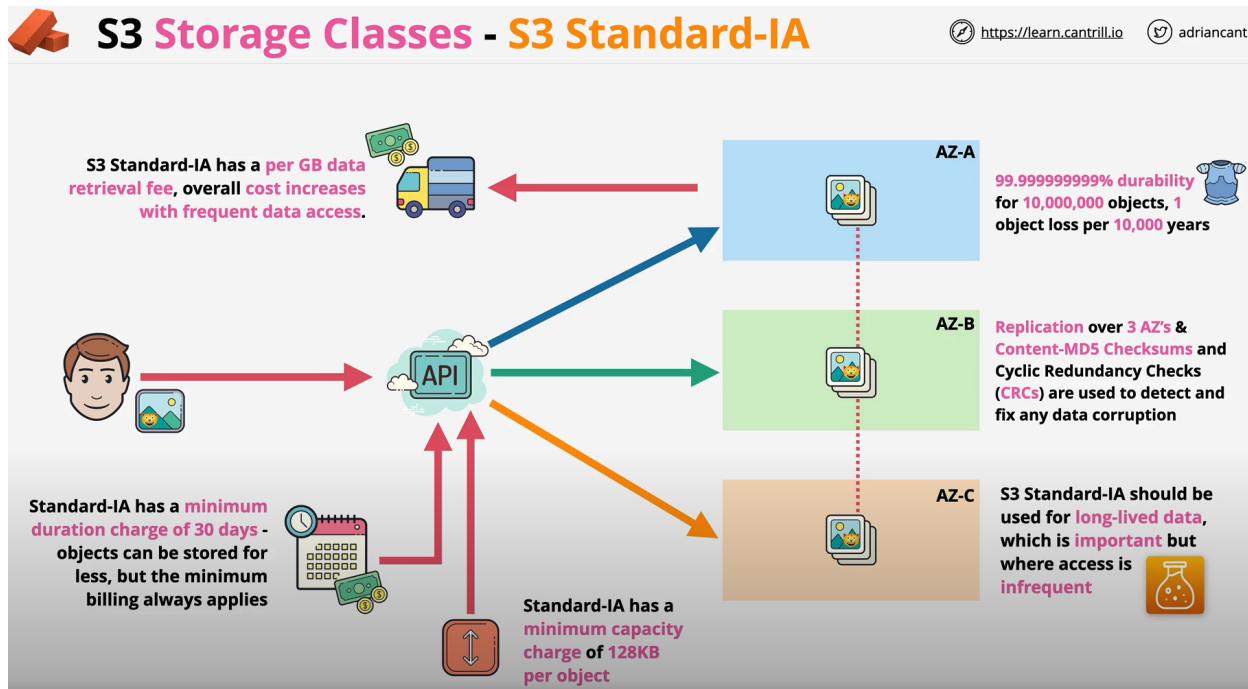
S3 Storage Classes - S3 Standard

<https://learn.cantrill.io>

adriancantrr



S3 infrequent Access ()



much cheaper than standard S3

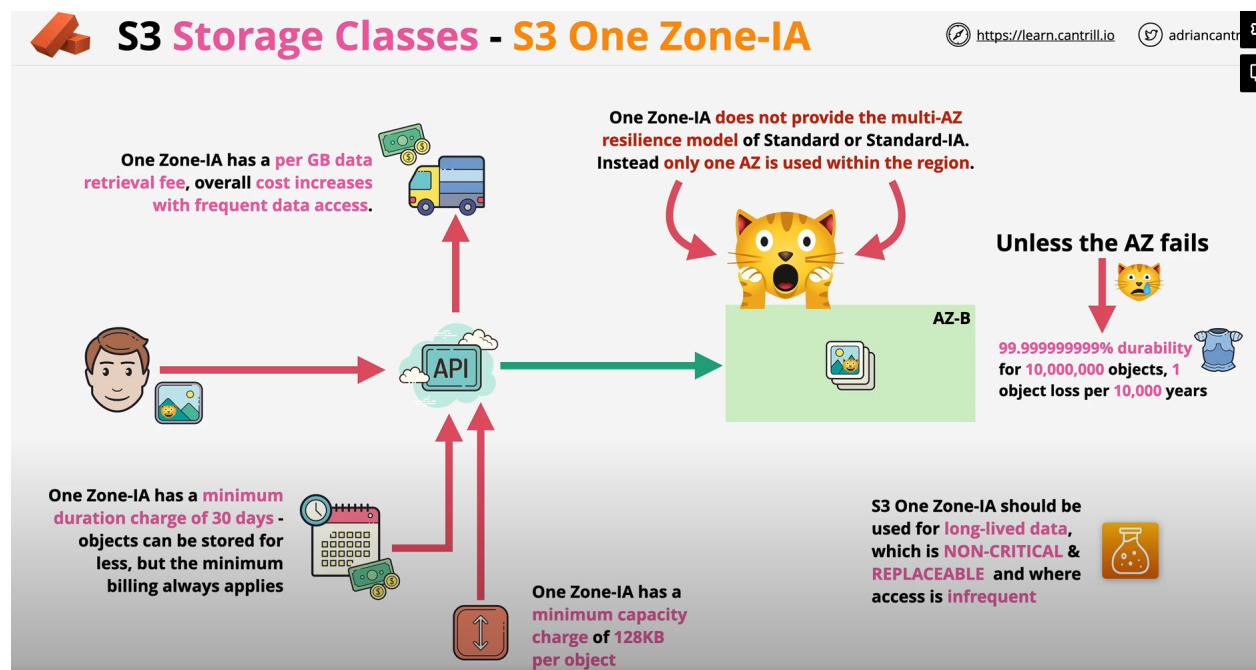
Compromises:

cost retrieval fee

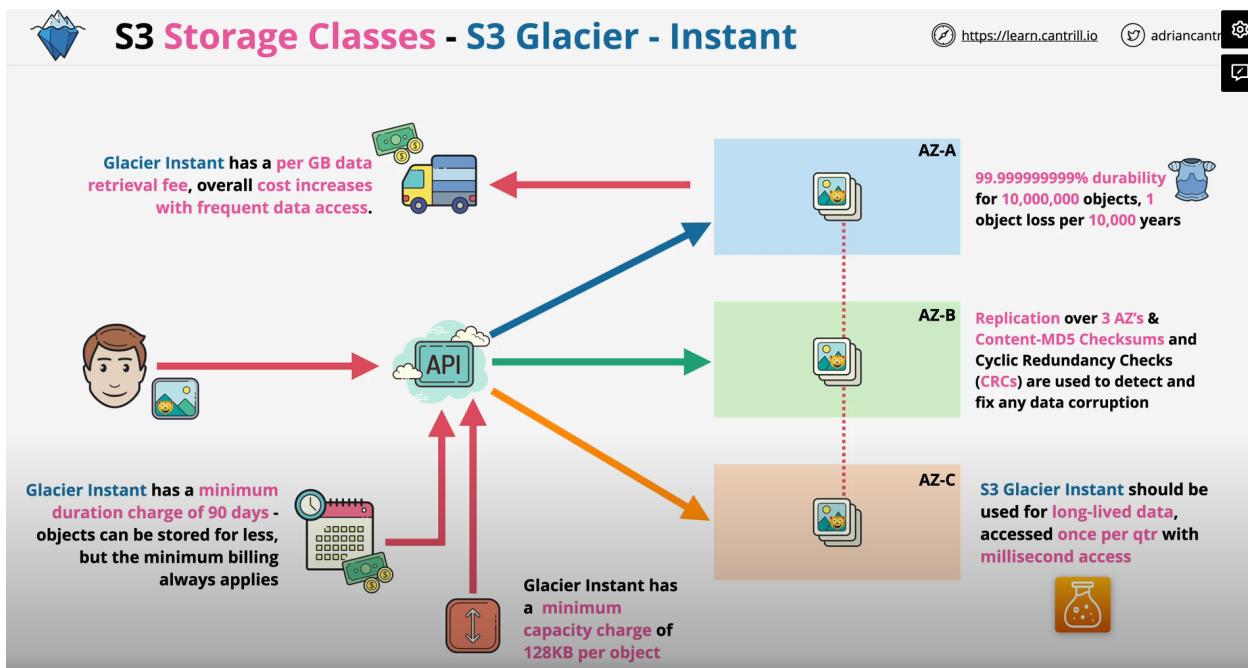
Cost effective for long-term data storage and for larger files

use it for not important storage

S3 One zone Infrequent access:



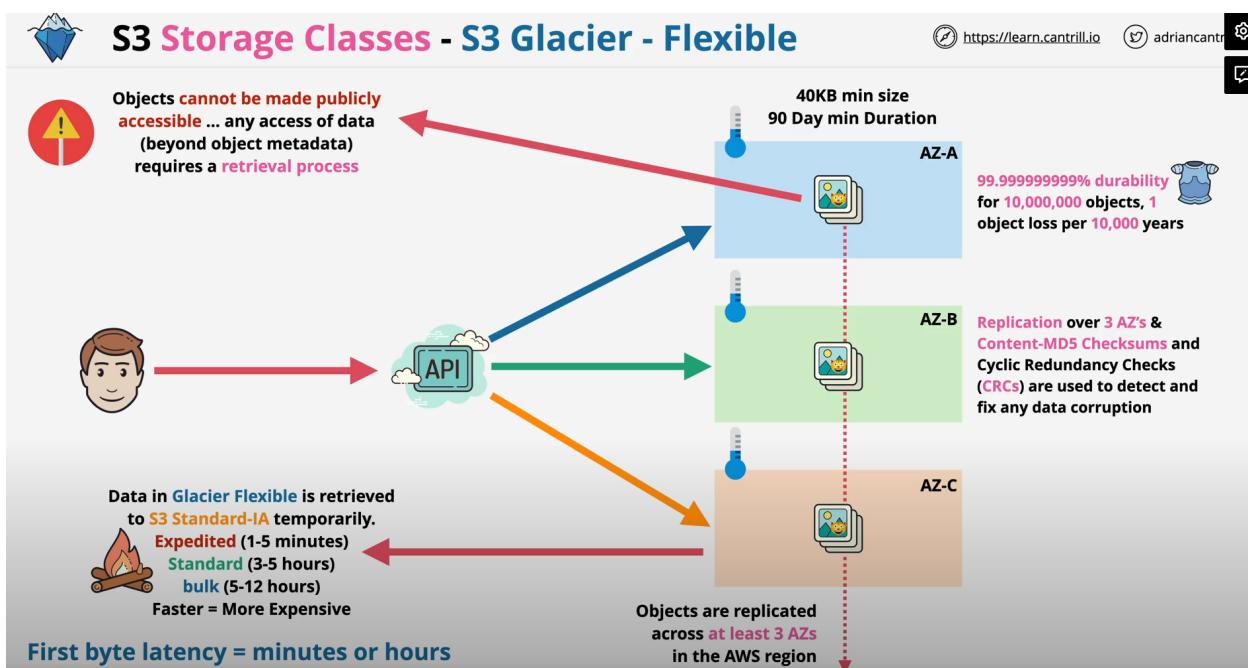
S3 Glacier Instant:



S3 Glacier Flexible:

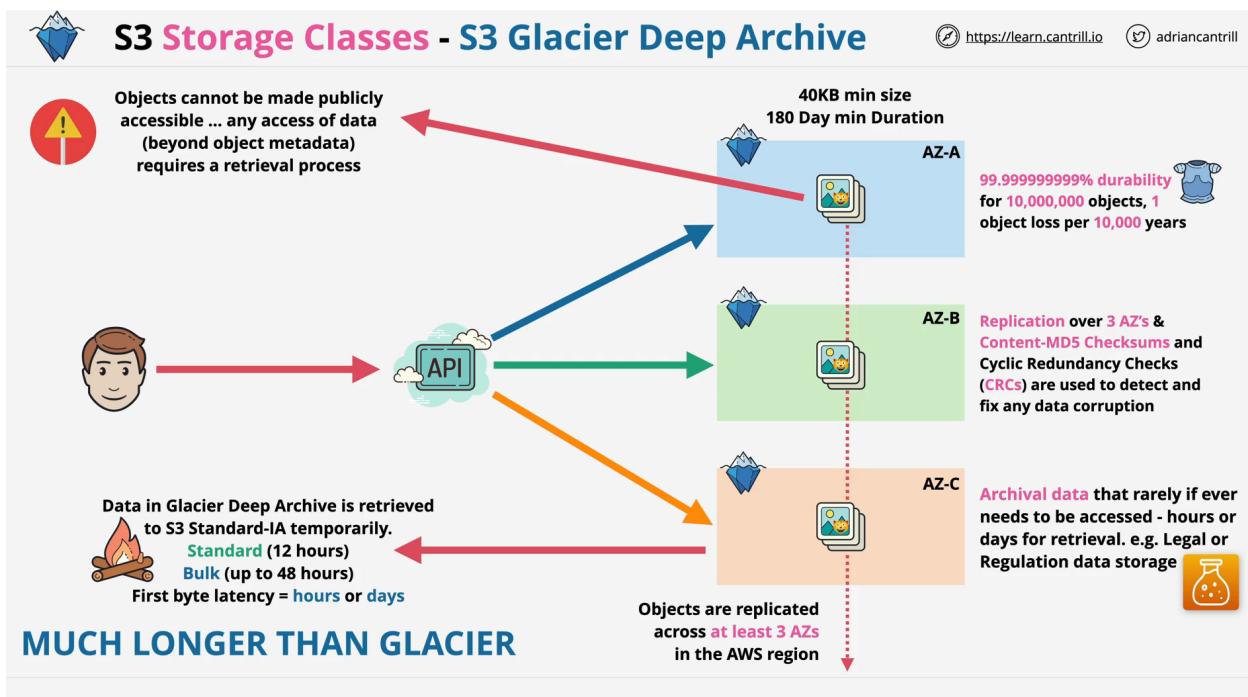
chill

usually used for archival data and one of the cheapest



S3 Glacier Deep Archive:

frozen state



Intelligent tiering:

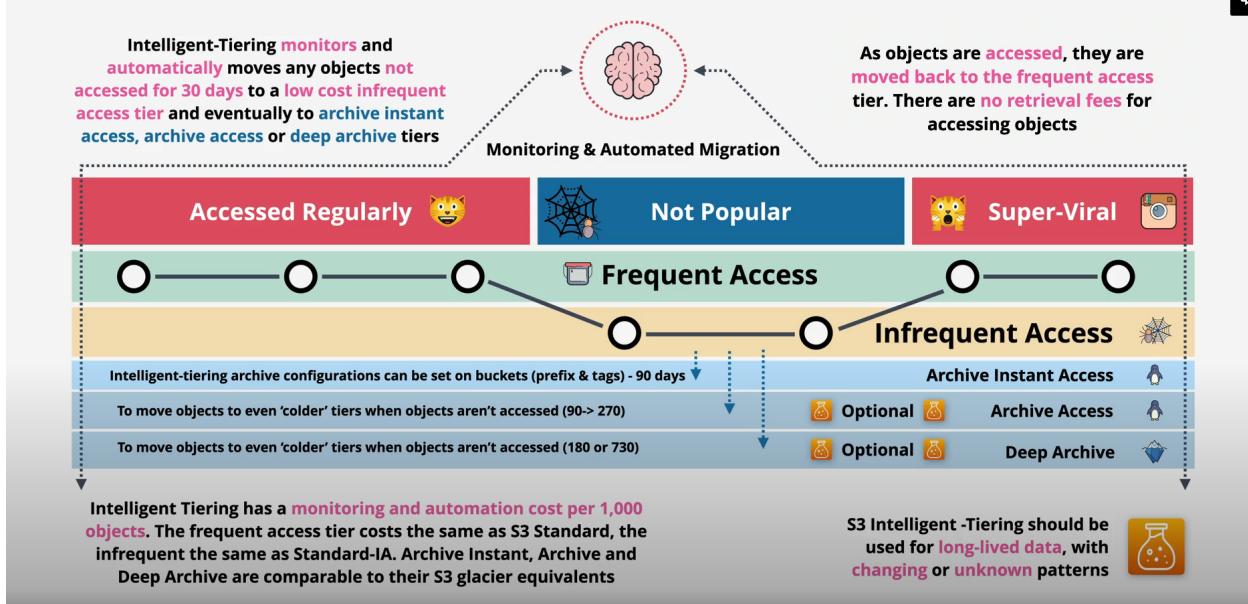
more costly because of management fees



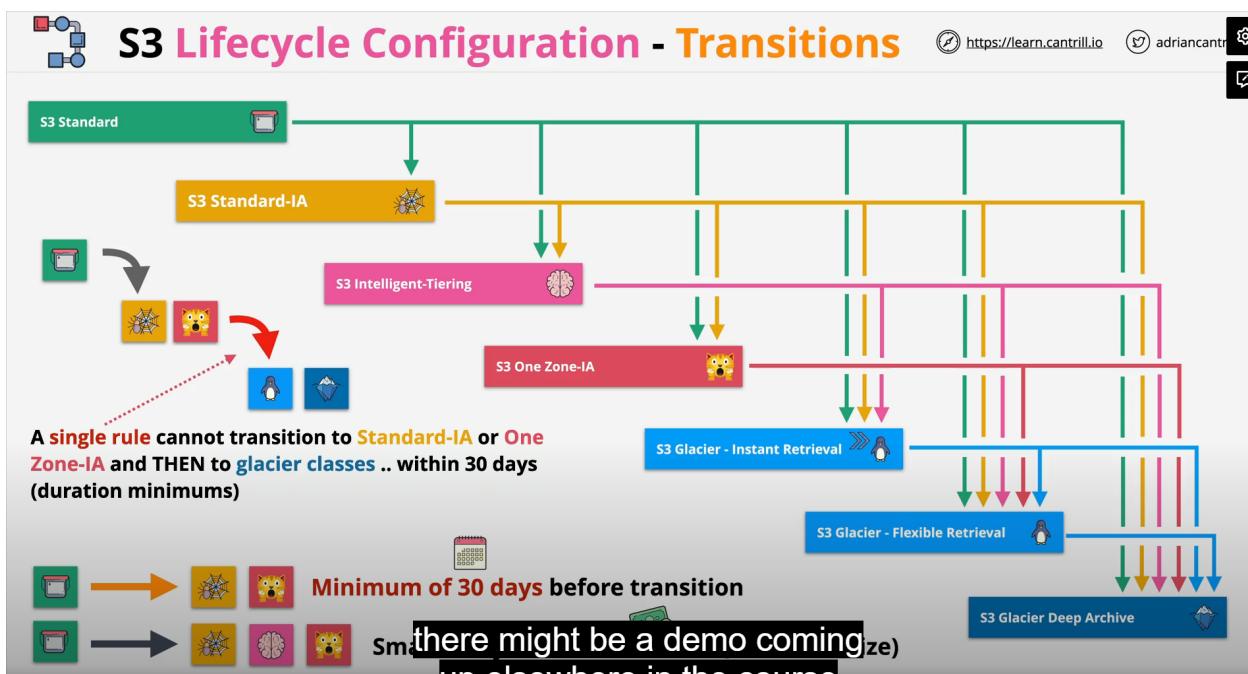
S3 Intelligent-Tiering

<https://learn.cantrill.io>

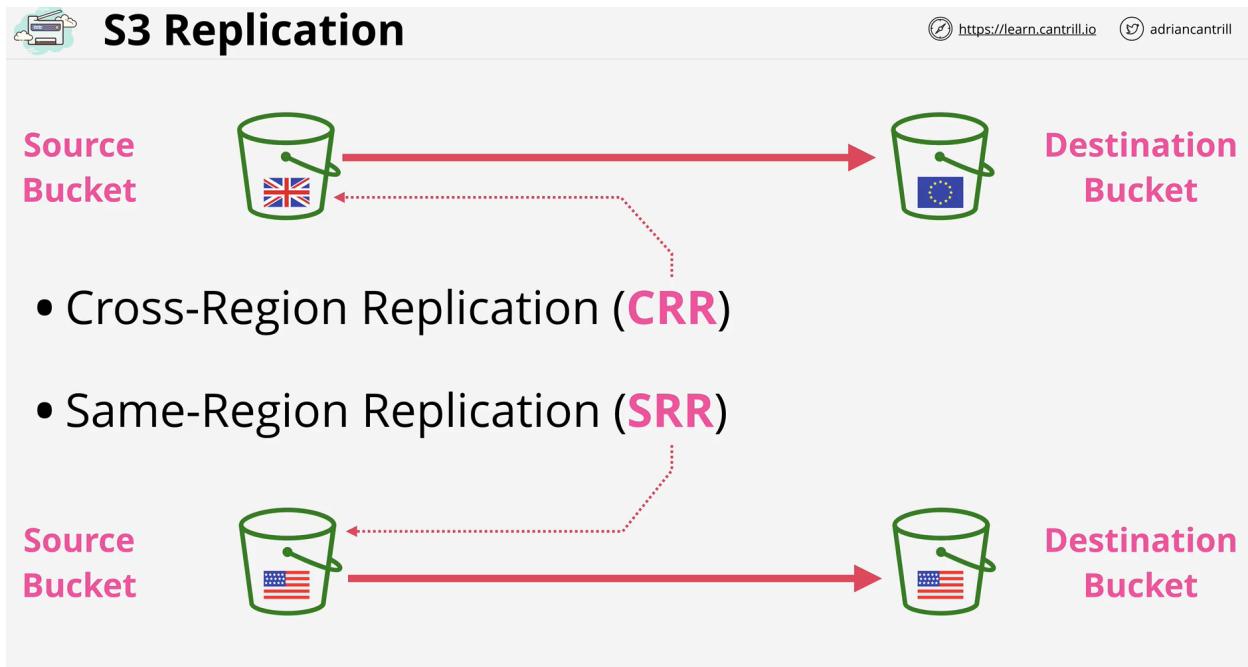
adriancantr

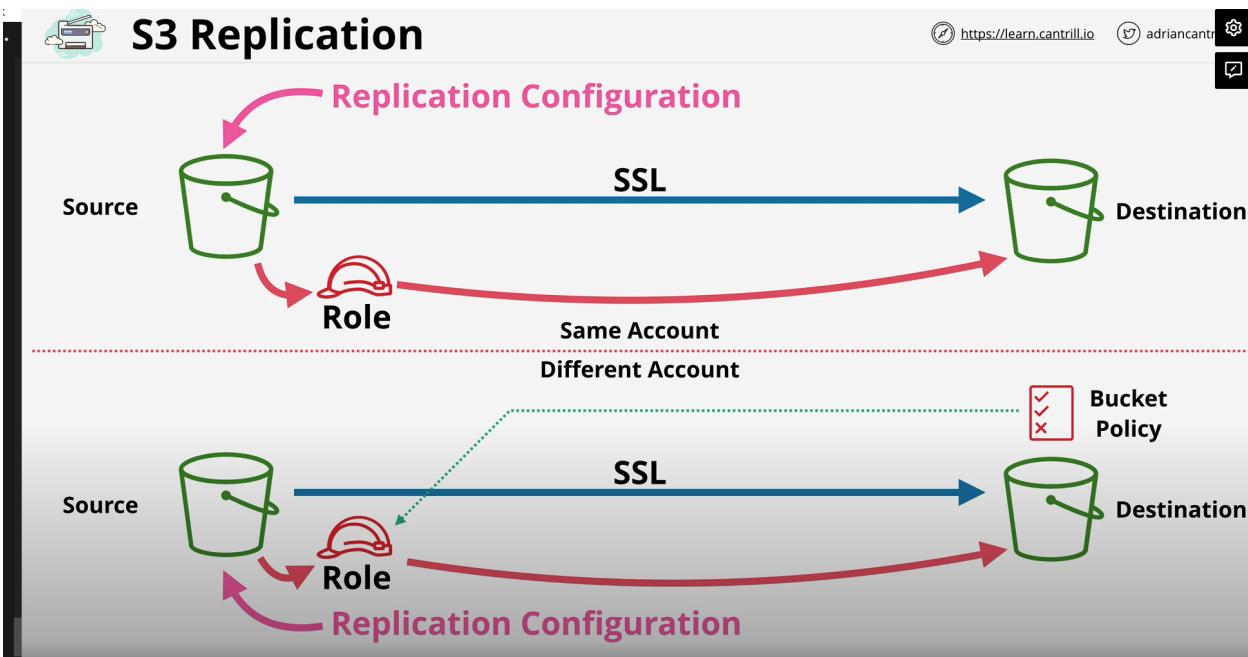


S3 lifecycle configuration:



S3 Replication:





What to replicate??

it is better to use same s3 class as original file when replicating data to new destination
for ex. (S3 storage IA)

but you can overwrite that

you also have to define ownership of account

RTC: Replication time control

15 min time control



S3 Replication Options

<https://learn.cantrill.io>

adriancantrill



- All objects or a subset
- Storage Class - default is to maintain
- Ownership - default is the source account
- Replication Time Control (RTC)

IMP:

not retroactive which means lets say I start the replication on the bucket today which means from today onwards only the data will be replicated to new destination not the previous data.

Versioning should be enabled on both of the buckets

One way replication only

cannot replicate SSE-C (because doesn't have customer key)

no glacier or deep archive can be replicated

deletes cannot be replicated



S3 Replication Considerations

<https://learn.cantrill.io>

adriancantr

- **Not retroactive** & Versioning needs to be **ON**
- **One-way replication** Source to Destination
- Unencrypted, SSE-S3 & SSE-KMS (**with extra config**)
- Source bucket owner needs permissions to objects
- NO **system events, Glacier or Glacier Deep Archive**
- **NO DELETES**

WHY you use replication??



Why use replication..?



<https://learn.cantrill.io>



adria

- SRR - Log Aggregation
- SRR - PROD and TEST Sync
- SRR - Resilience with strict sovereignty
- CRR - Global Resilience Improvements
- CRR - Latency Reduction

DEMO:

Of replication.

Presigned url:

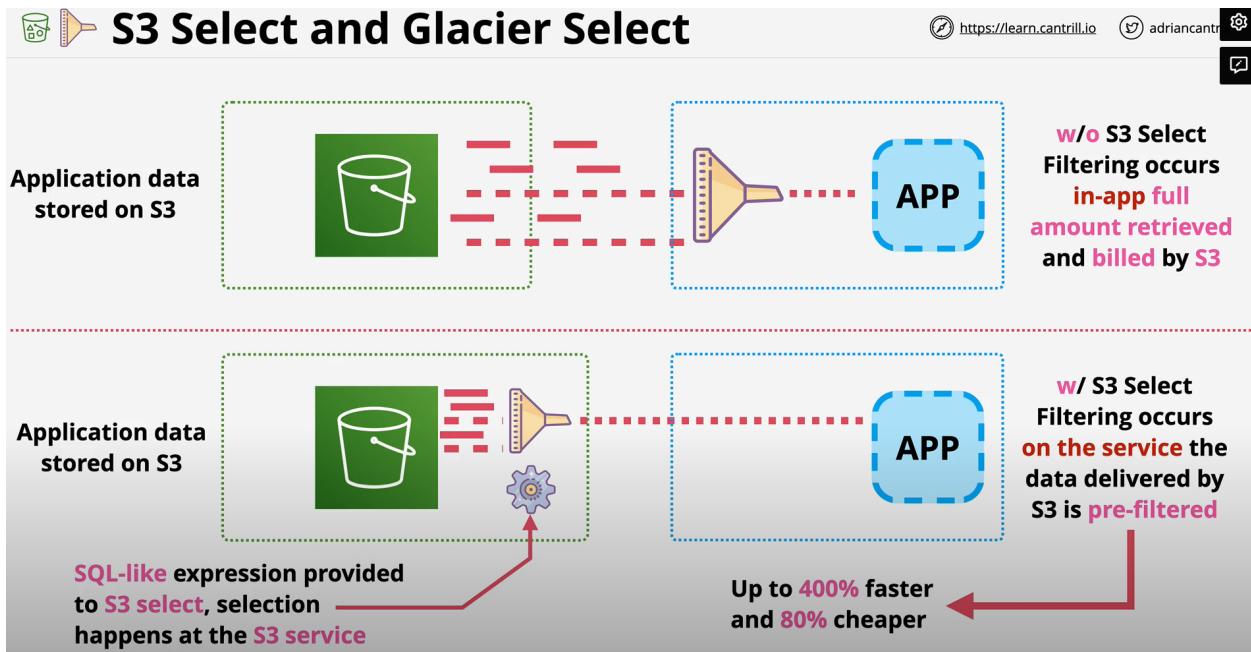
To give access to something selected with expiry

PresignedURLs

 https://learn.cantrill.io  adriancantr 

- You can create a URL for an object you have **no access to**
- When using the URL, the permissions match the **identity which generated it ..**
- Access denied could mean the generating ID **never had access** .. or **doesn't now**.
- **Don't generate with a role** .. URL stops working when temporary credentials expire...

S3 select and Glacier Select



S3 EVENT Notification:

S3 Event Notifications

https://learn.cantrill.io adriancantrill

- **Notification** generated when **events** occur in a **bucket**
- .. can be delivered to **SNS**, **SQS** and **Lambda** Functions
- Object **Created** (Put, Post, Copy, CompleteMultiPartUpload)  
- Object **Delete** (*, Delete, DeleteMarkerCreated)
- Object **Restore** (Post (Initiated), Completed)  
- **Replication** (OperationMissedThreshold, OperationReplicatedAfterThreshold, OperationNotTracked, OperationFailedReplication)  

S3 Access Logs:



S3 Access Logs

Press Esc to exit full screen

<https://learn.cantrill.io>

adriancantrill

