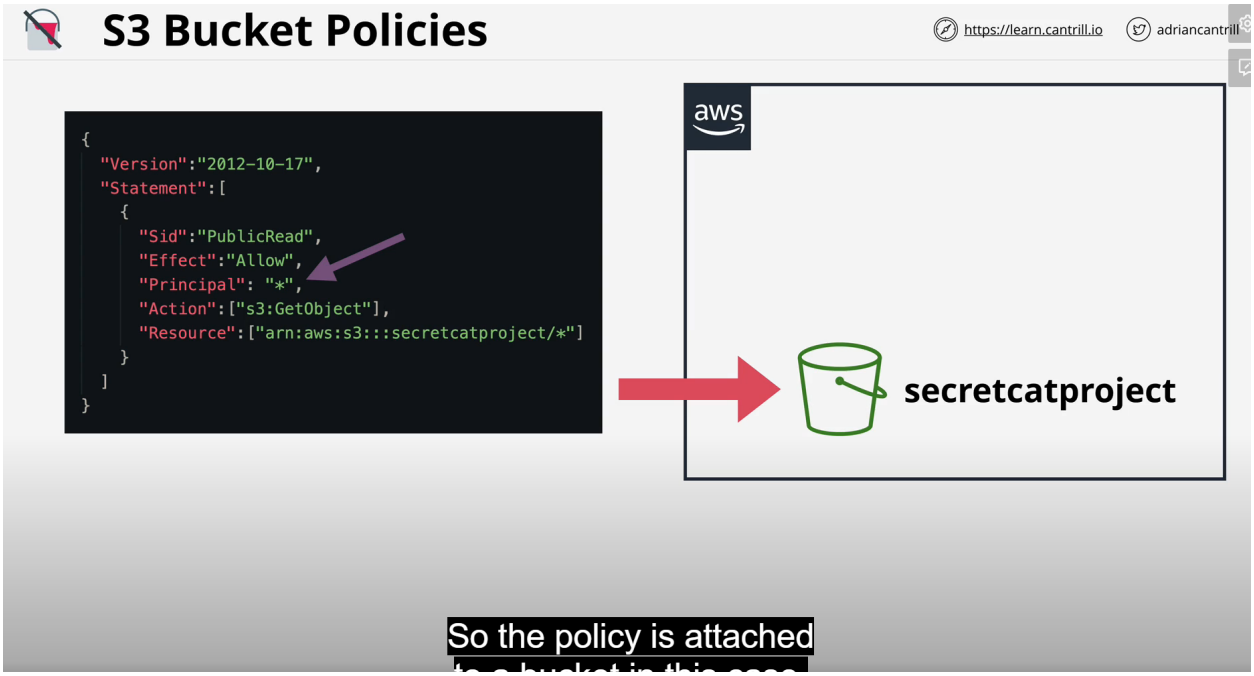
6. S3 Buckets

Created	@August 31, 2022 12:19 AM
Class	
Type	
Materials	
Reviewed	☐
Property	
Date	

S3 Bucket Policies

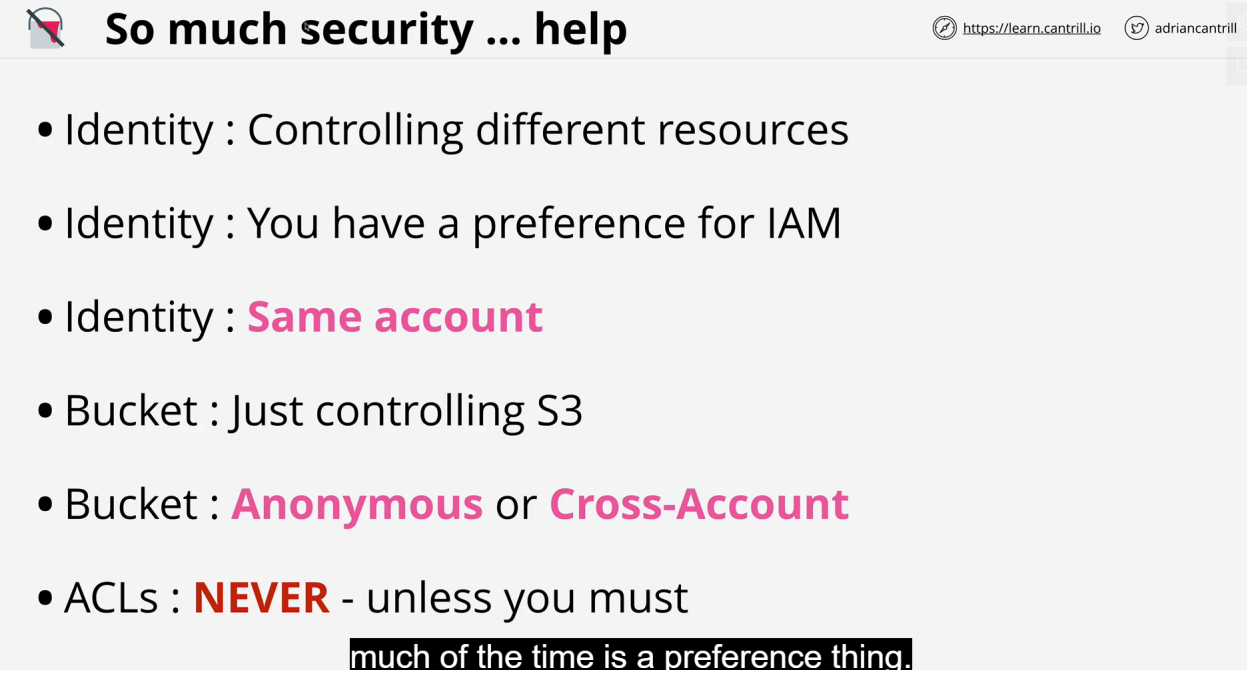
Resource Policies

Identity policy



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.

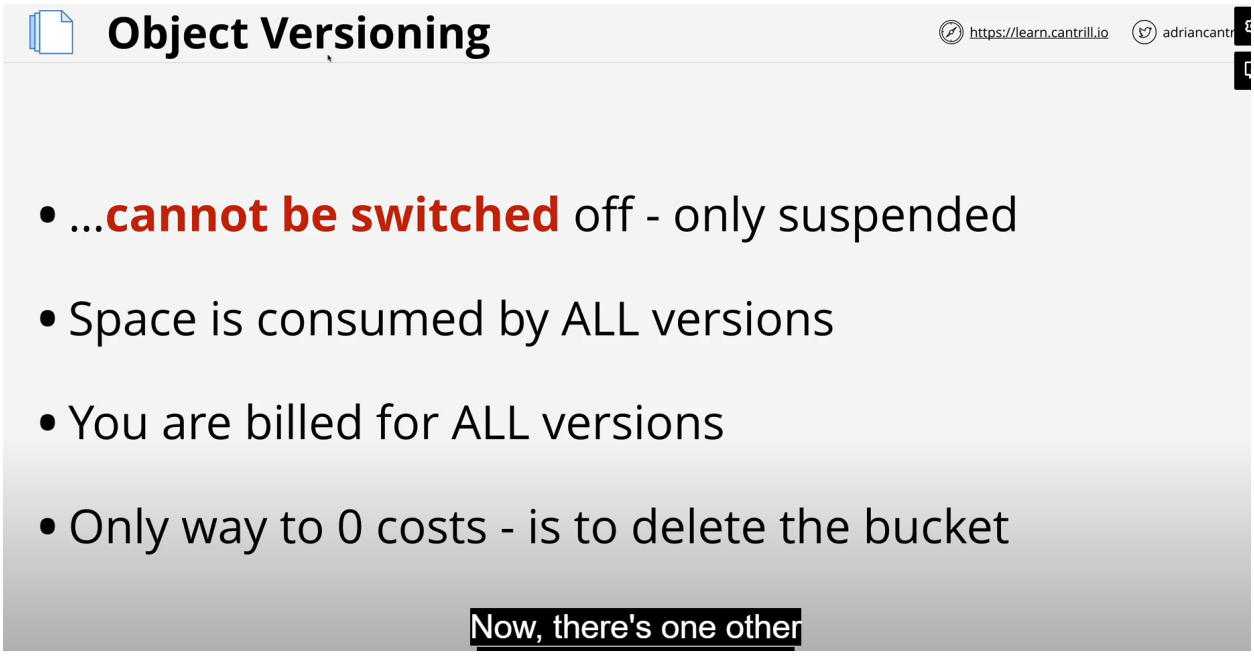


S3 Static website hosting and demo

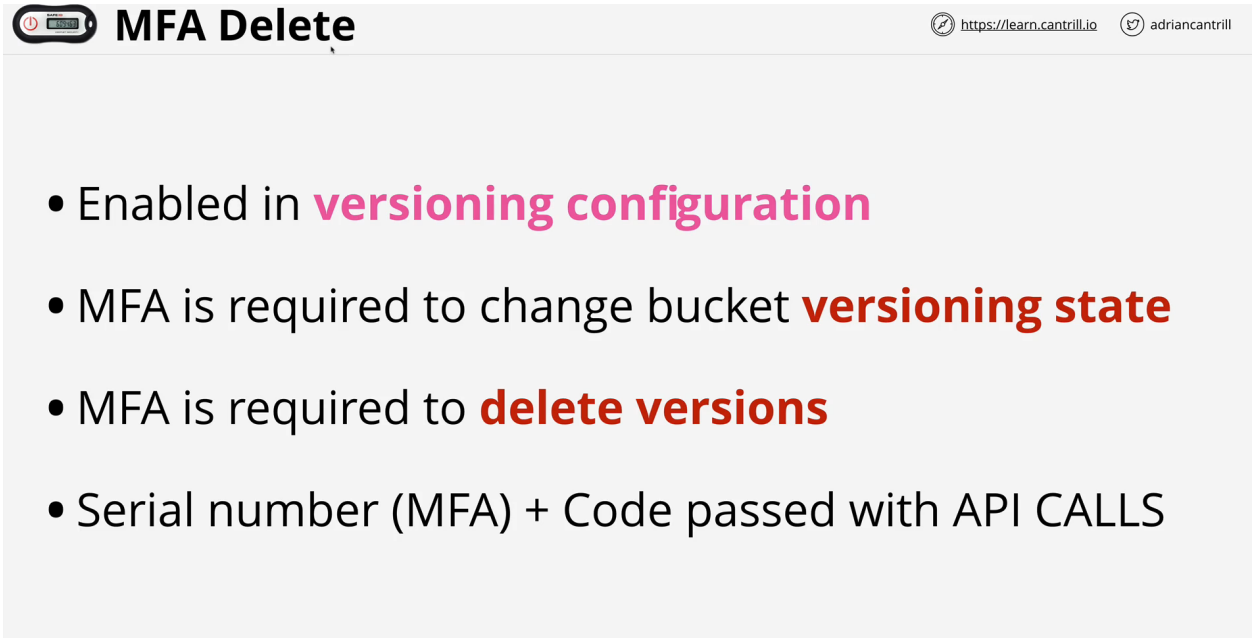
Done

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
adriancantr
• ...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 iteself 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

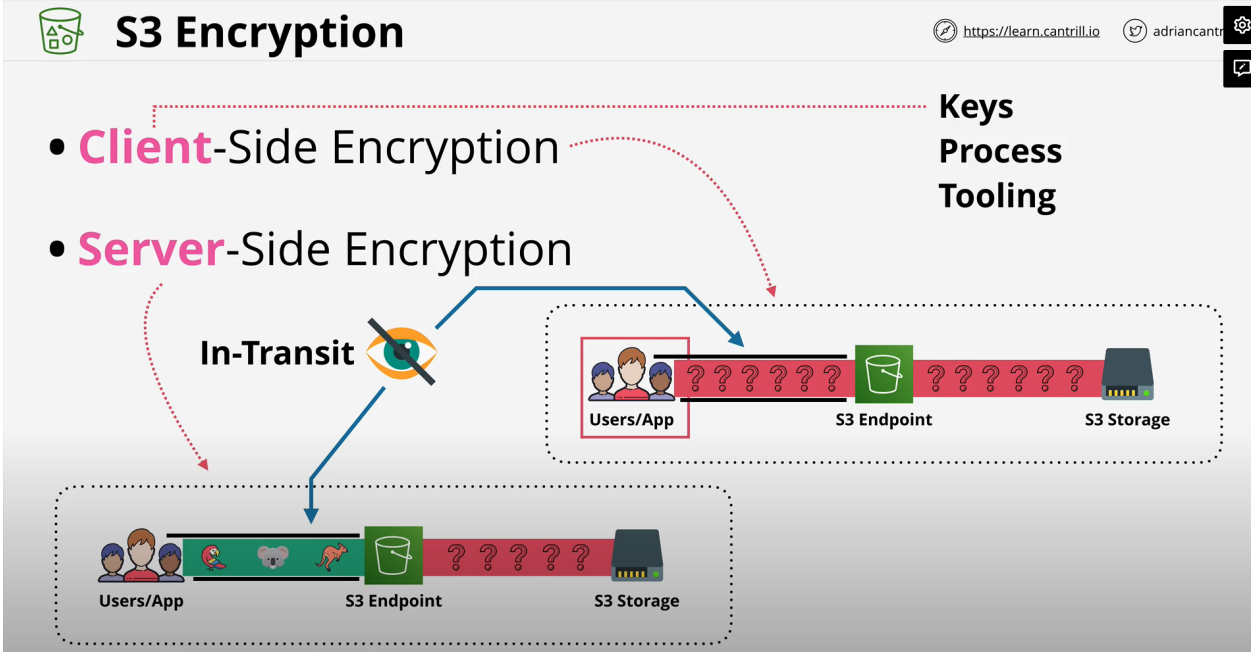
s3 see it as scrambled data

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:

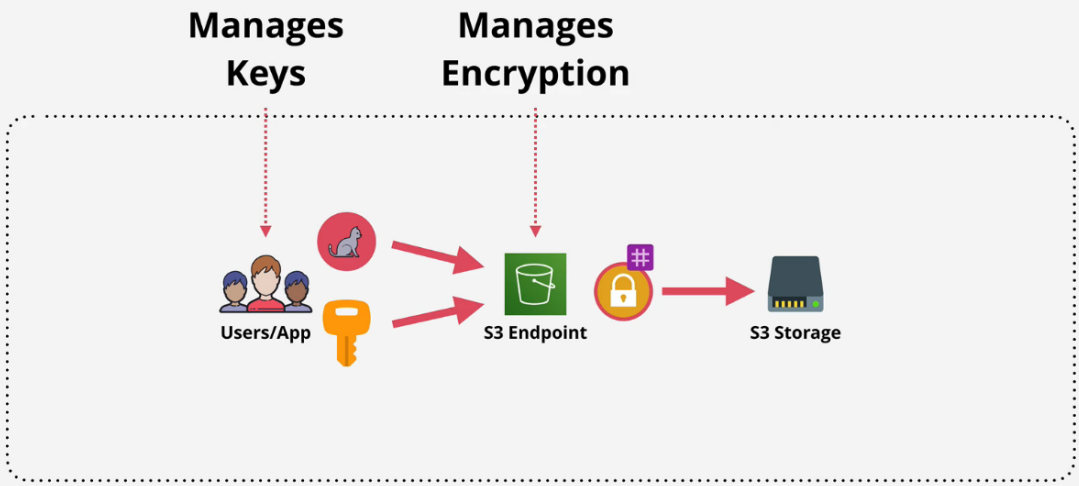
S3 Encryption

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 adrian

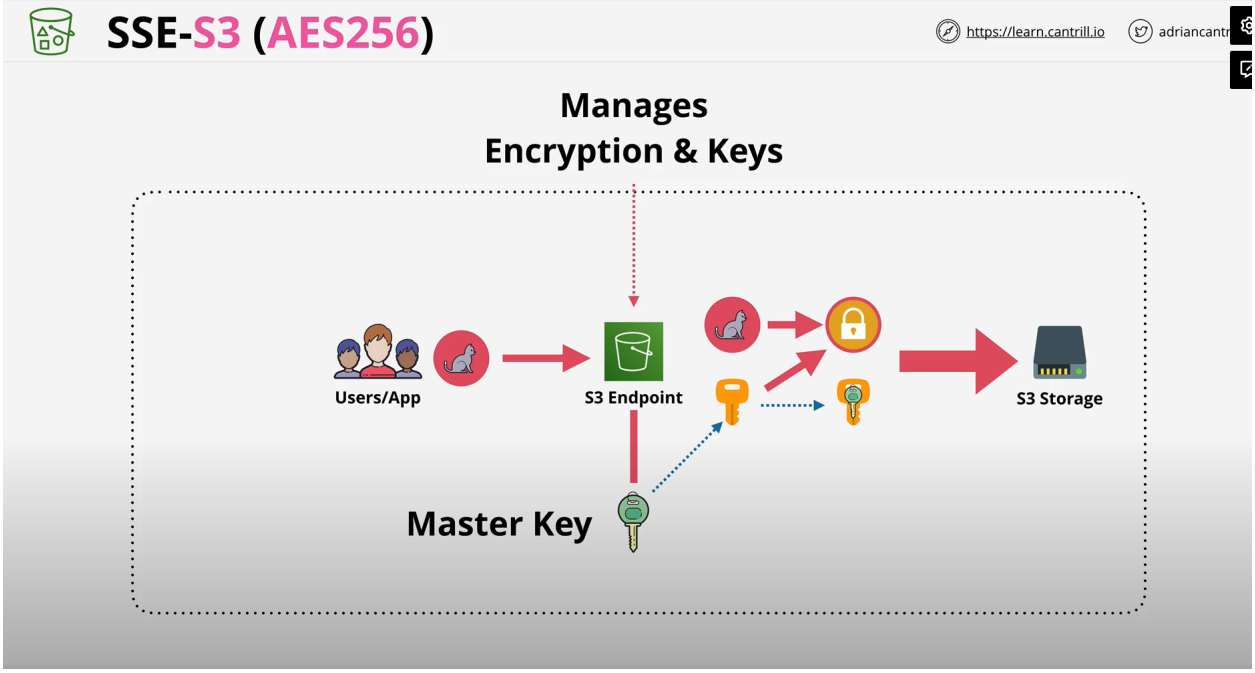


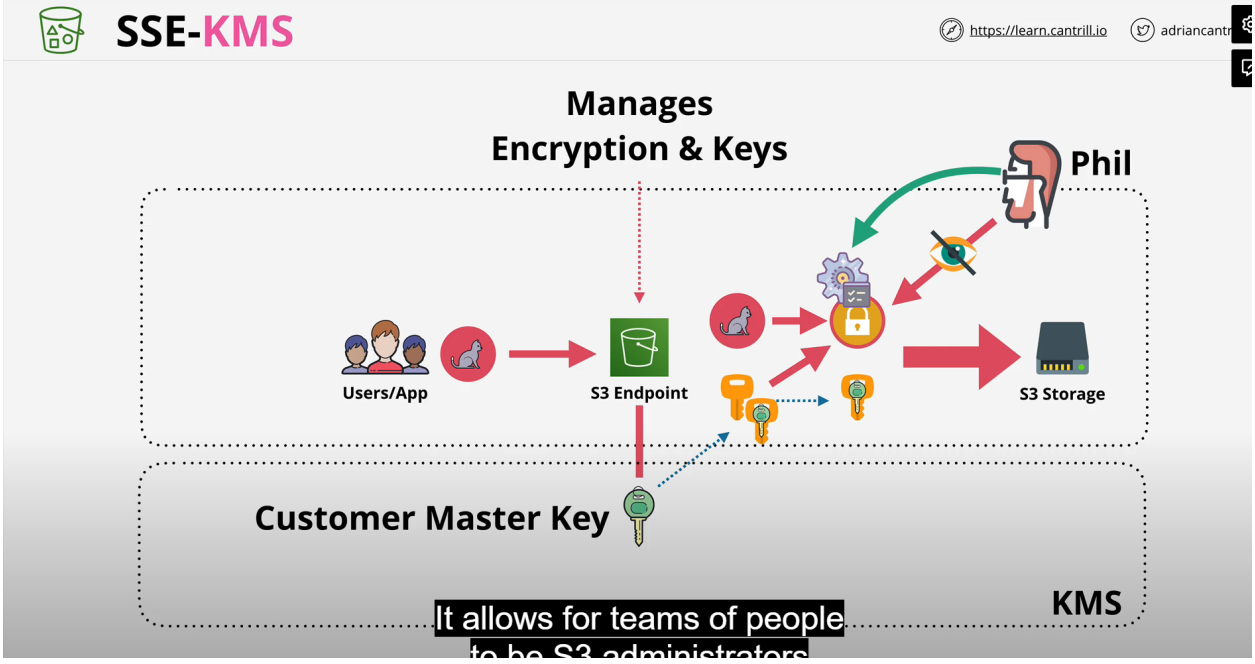
SSE-S3

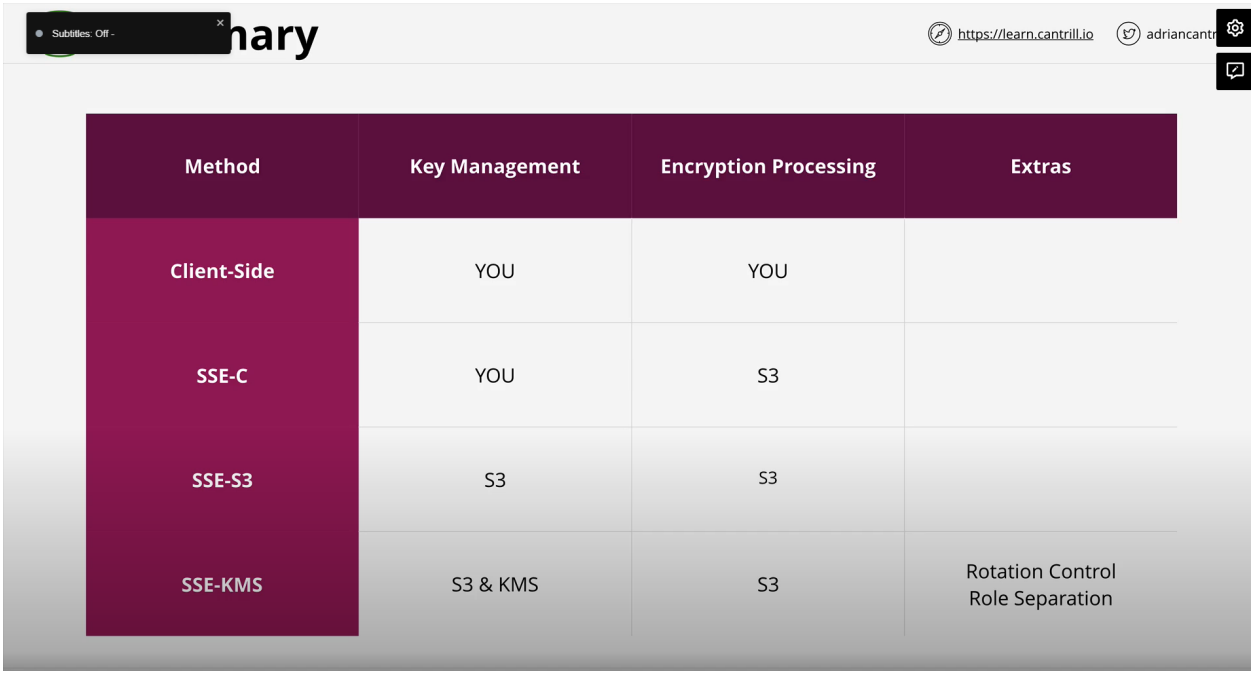
Not able to control the keys by user

admin dont have much control over key as aws handles the key

[USES AES 256 Encryption algorithm]

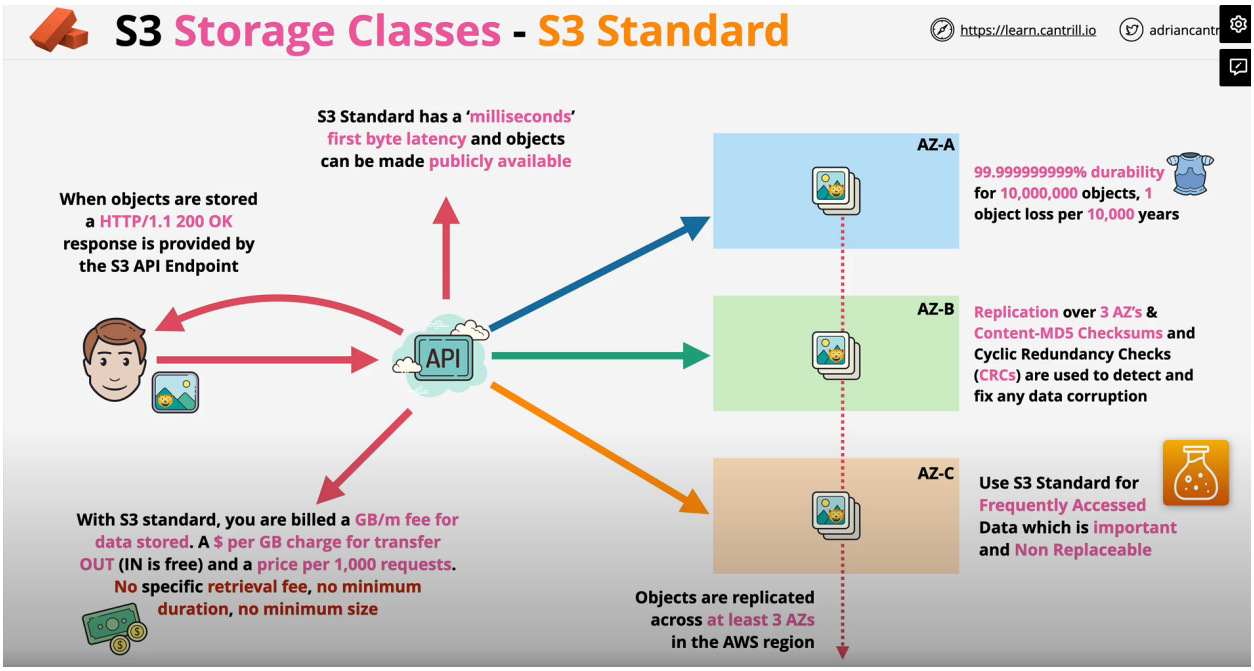




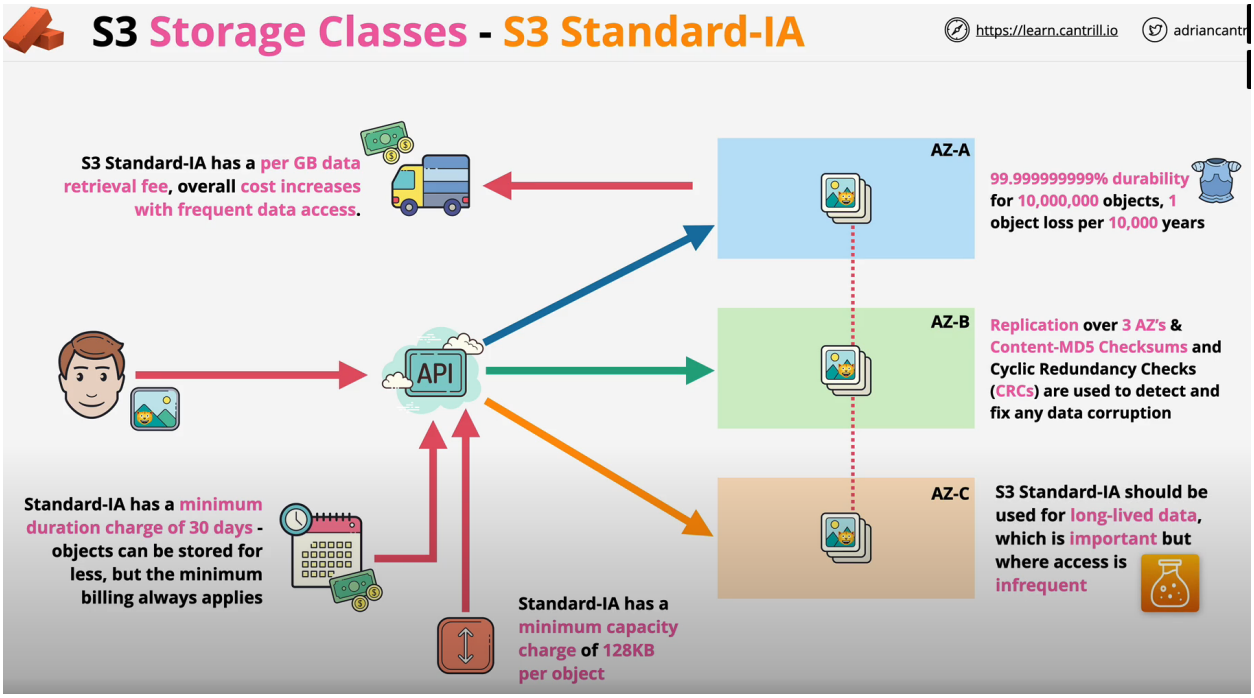


S3 Storage Classes:

s3 standard:



S3 infrequent Access ()



much searcher than standard s3

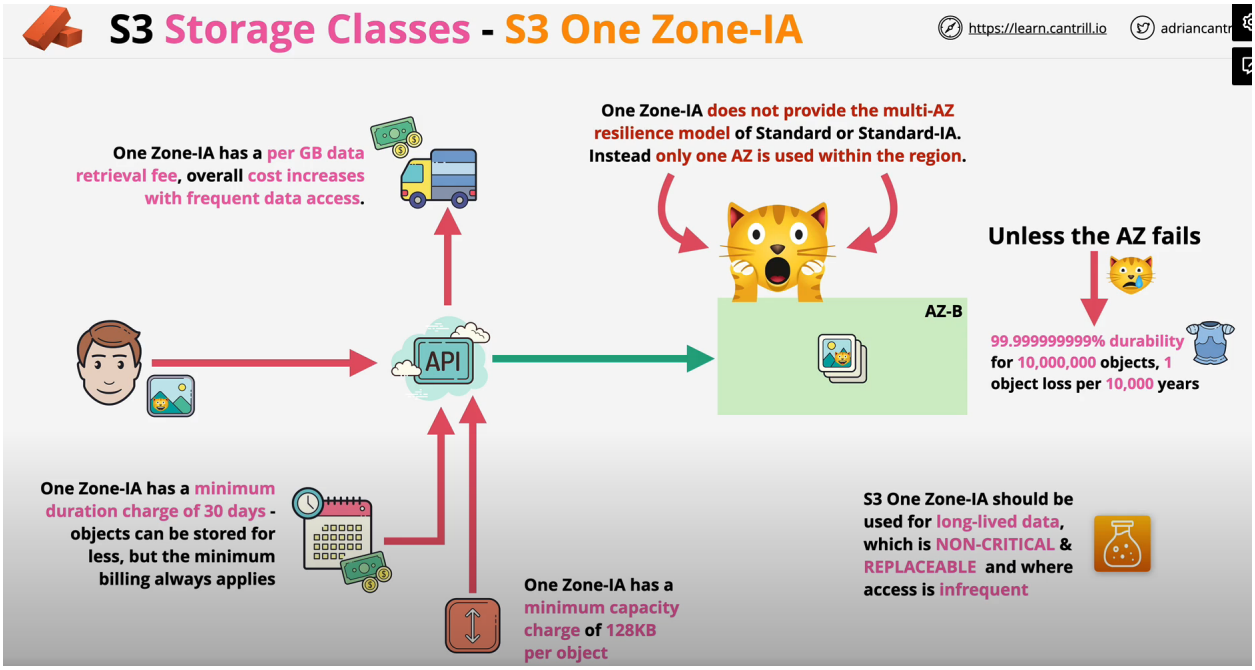
compromises:

cost retrieval fee

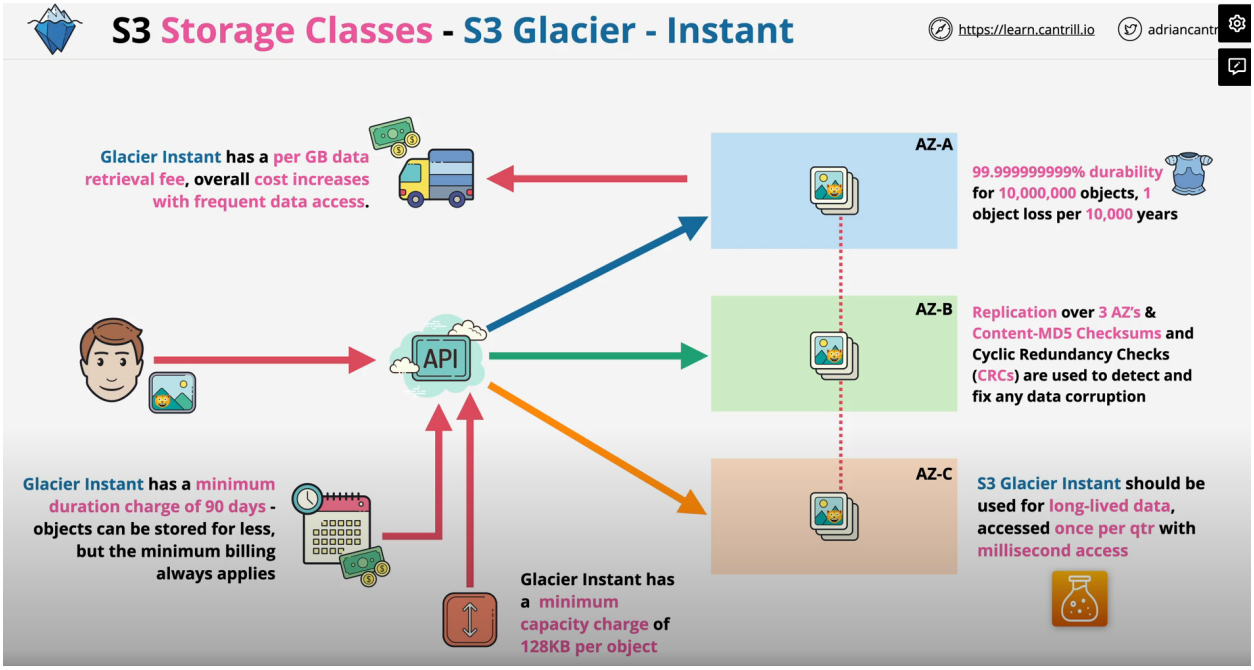
cost effective for long-term data storage and for larger files

use it for not important storage

S3 One zone Infrequent access:



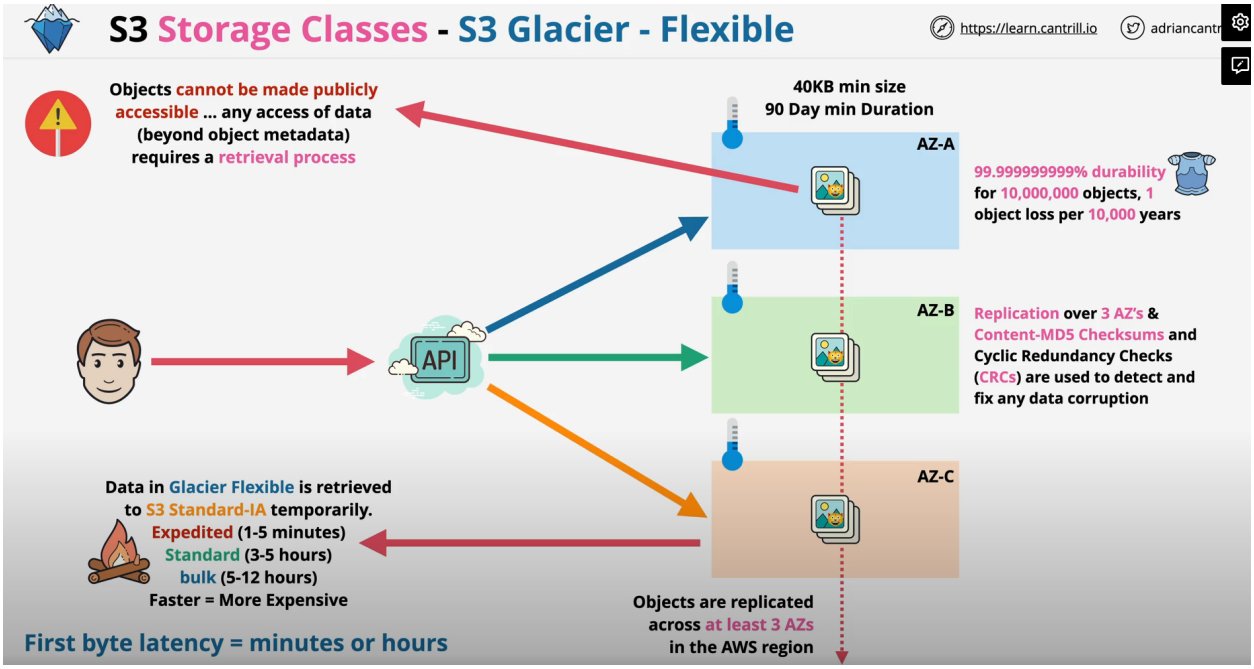
S3 Glacier Instant:



S3 Glacier Flexible:

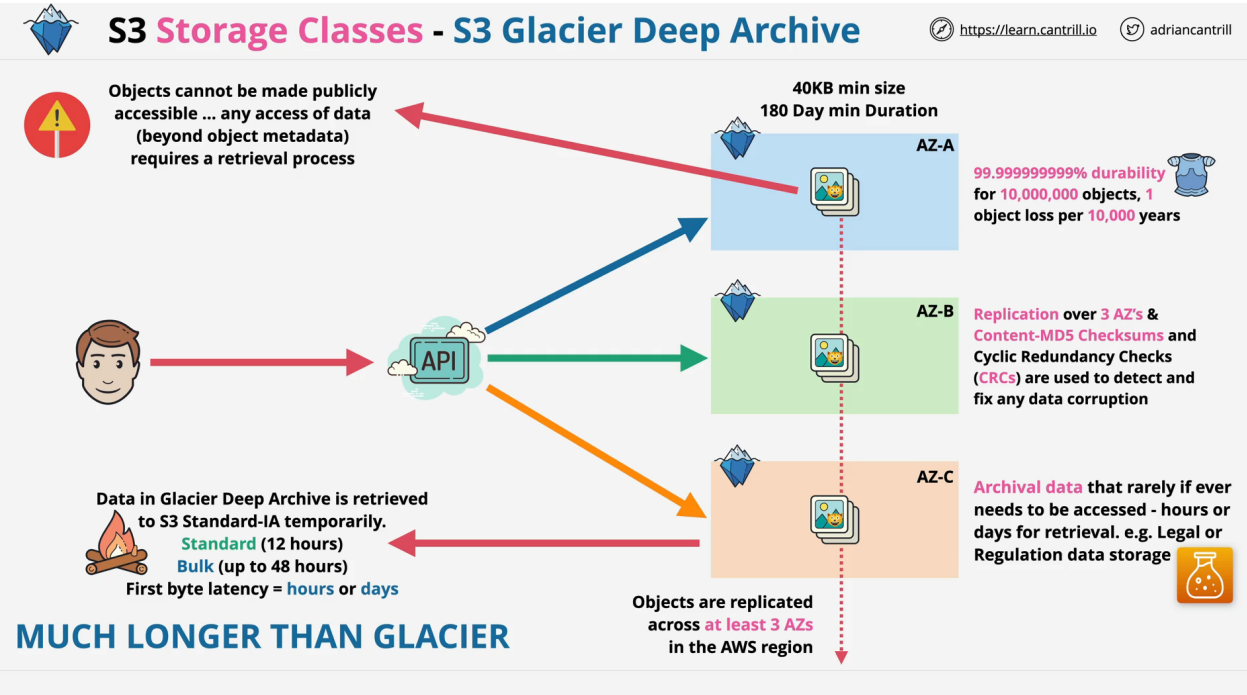
chill

usually used for archival data and one of the cheapest



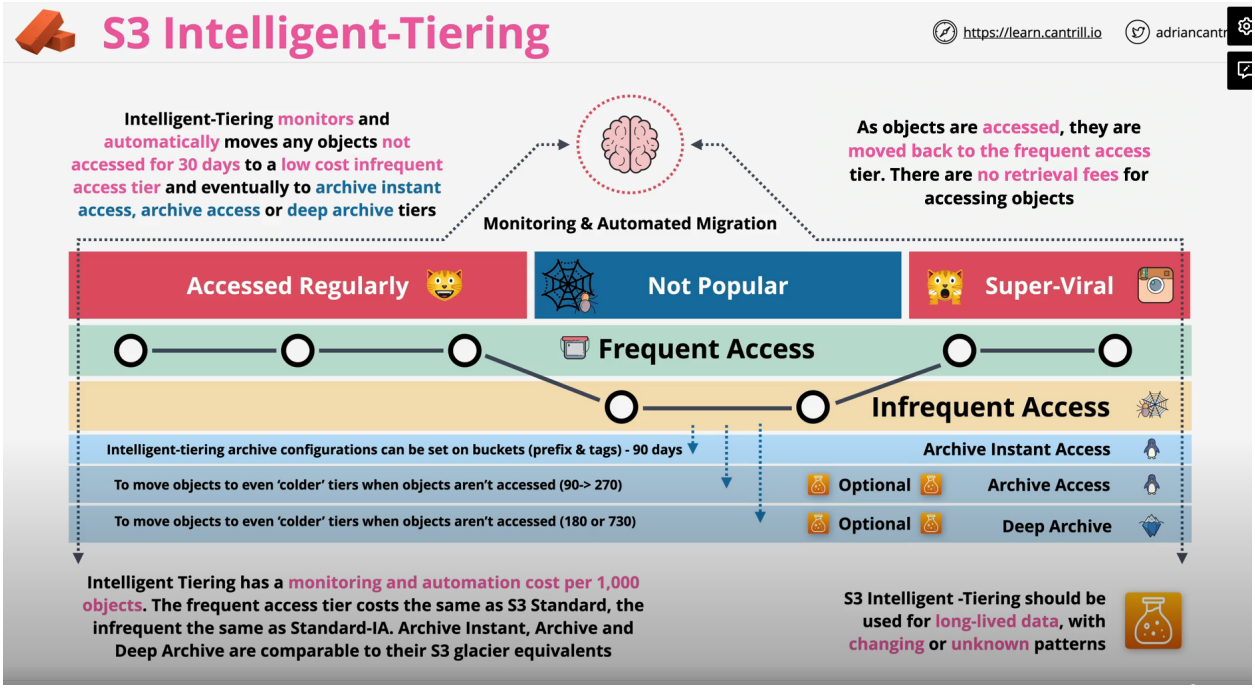
S3 Glacier Deep Archive:

frozen state

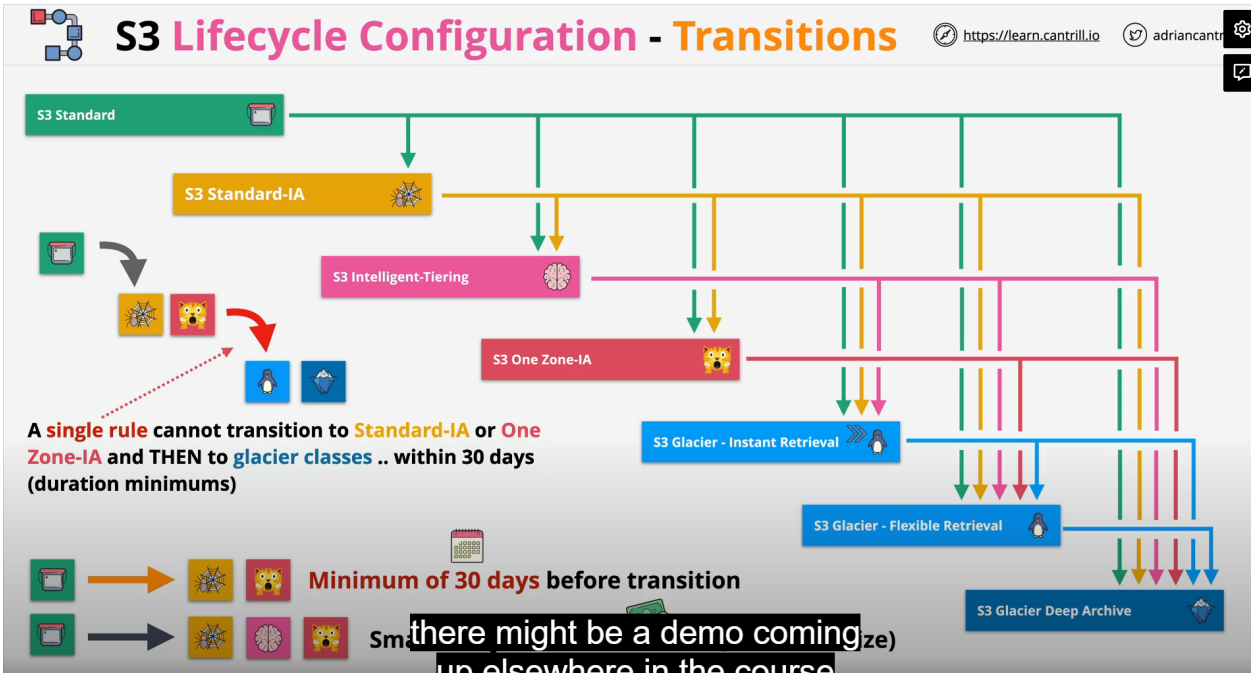


Intelligent tiering:

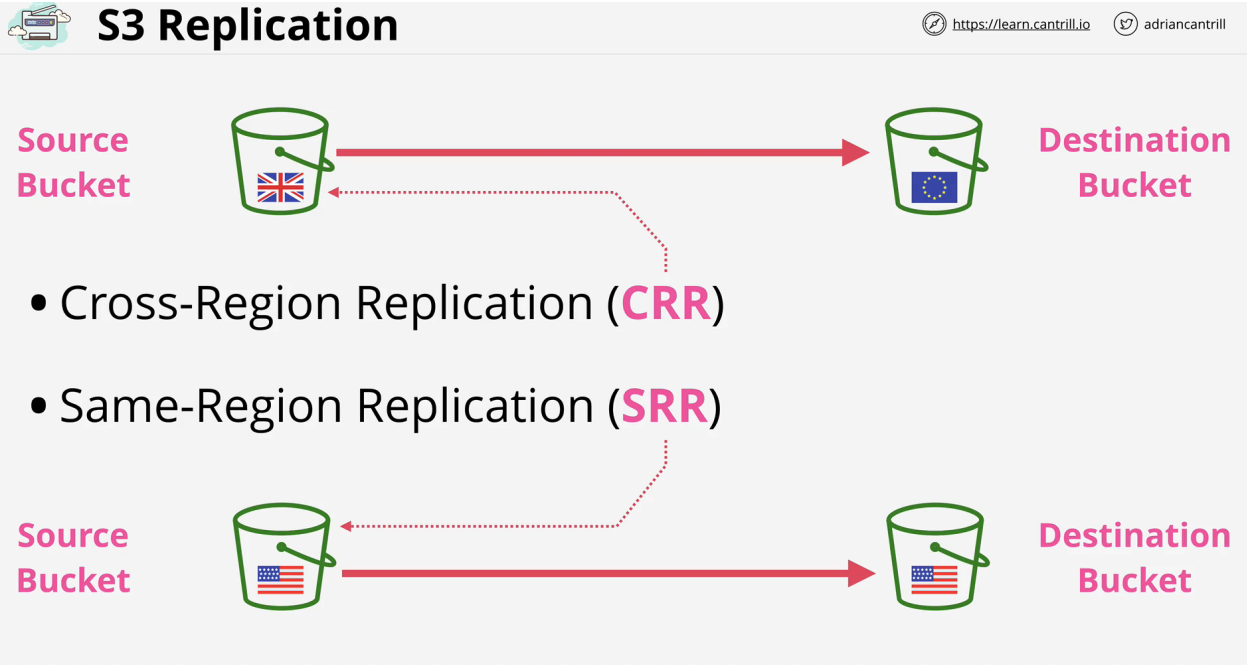
more costly because of management fees

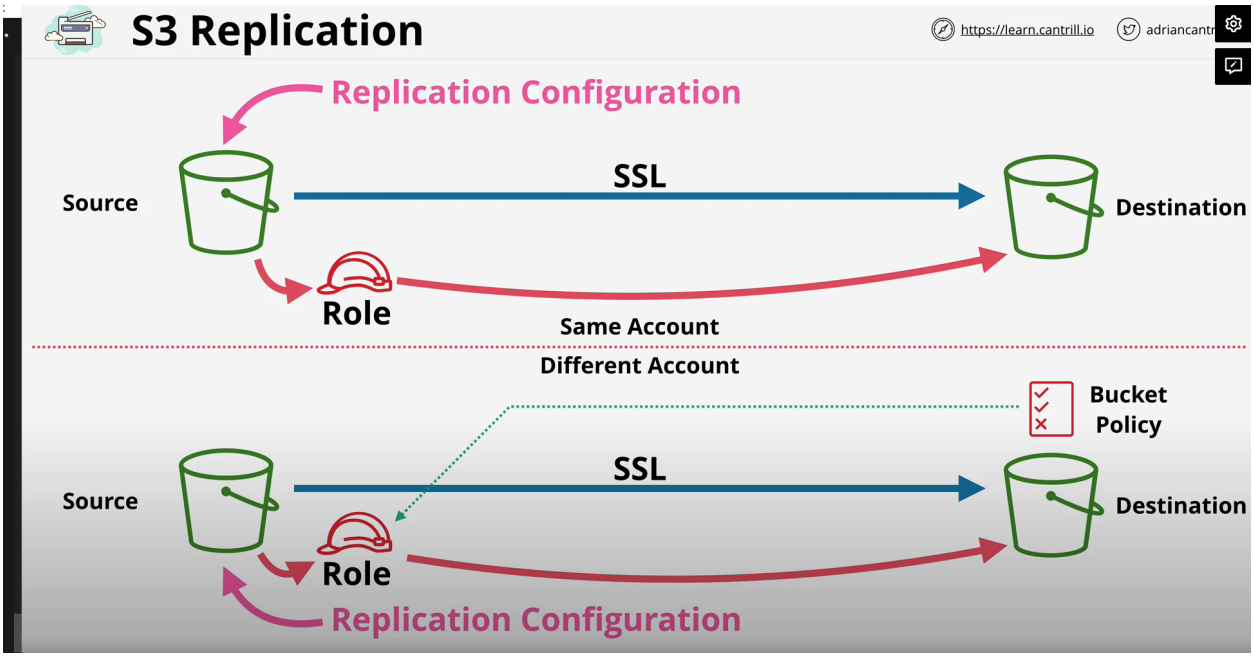


S3 lifecycle configuration:



S3 Replication:





What to replicate??

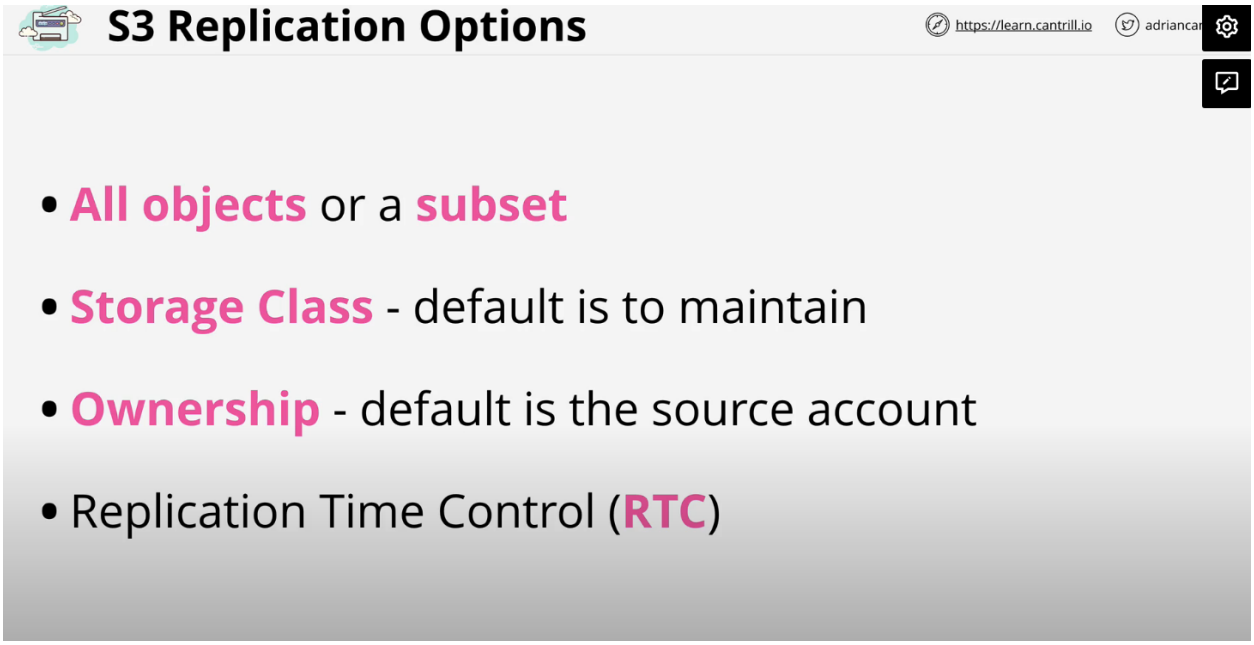
it is better to use same s3 class as original file when replicating data to new destination for ex. (S3 storage IA)

but you can overwrite that

you also have to define ownership of account

RTC: Replication time control

15 min time control



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.

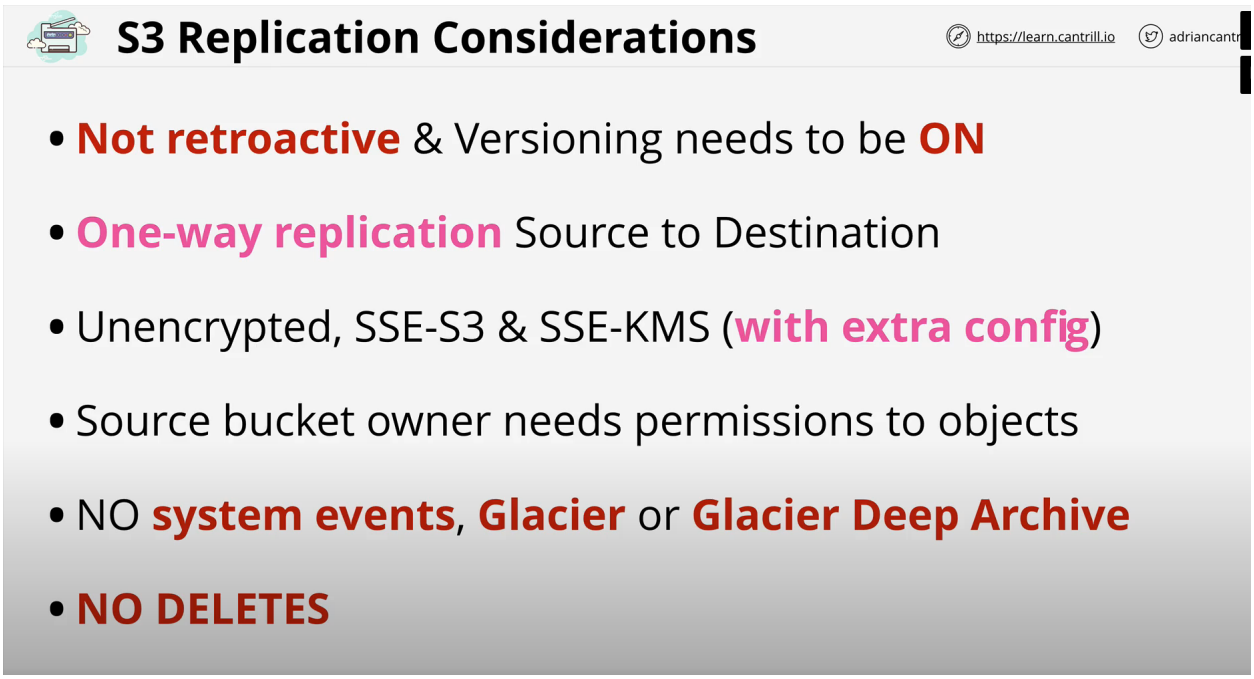
Versioning should be enabled on both of the buckets

One way replication only

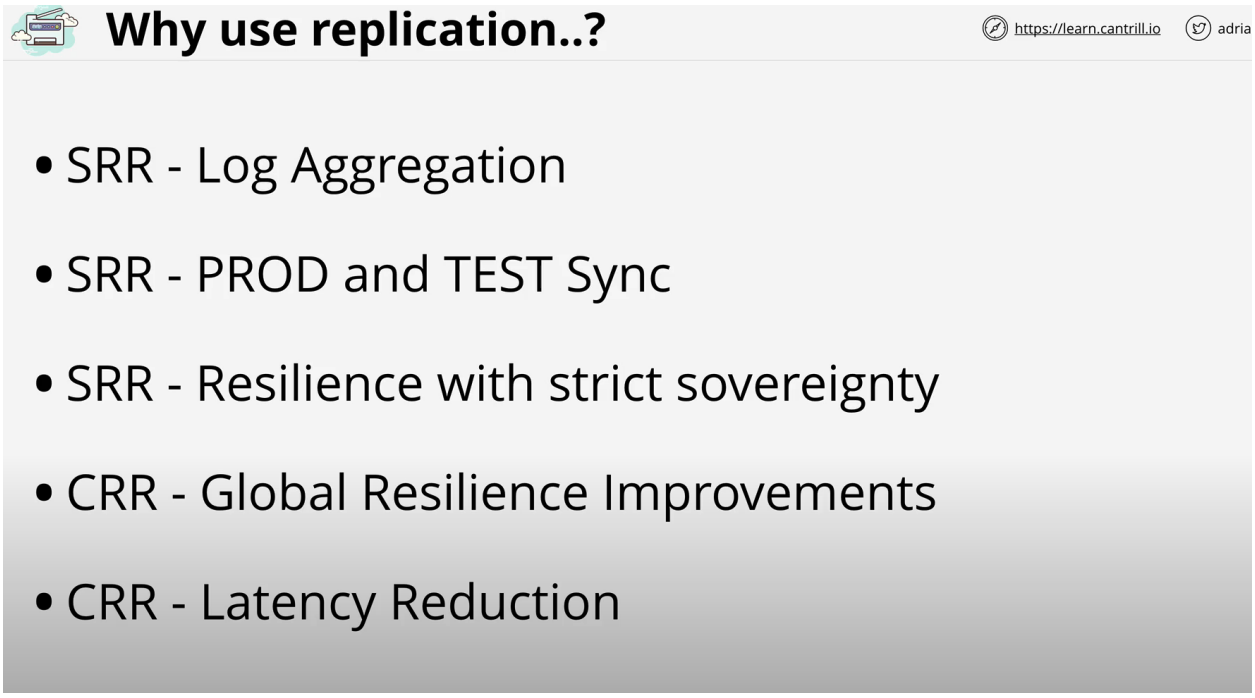
cannot replicate SSE-C (because doesn't have customer key)

no glacier or deep archive can be replicated

deletes cannot be replicated



WHY you use replication??



DEMO:

Of replication.

Presigned url:

To give access to something selected with expiry

PresignedURLs

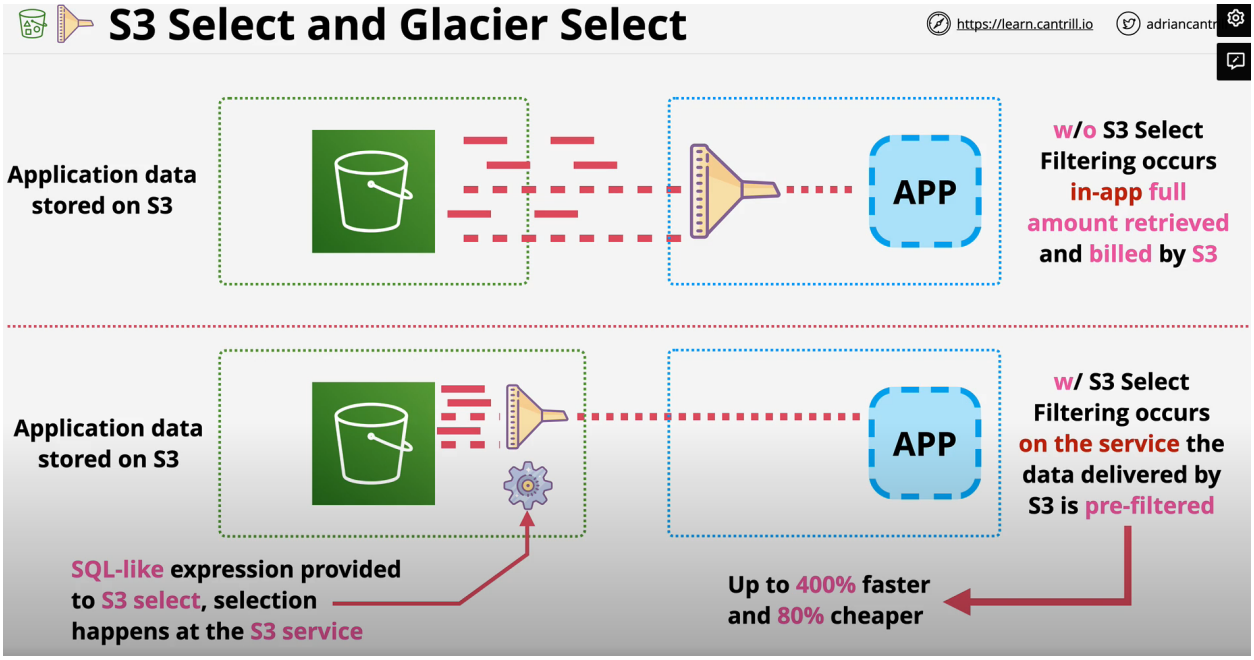
https://learn.cantrill.io adriancantr

- 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...

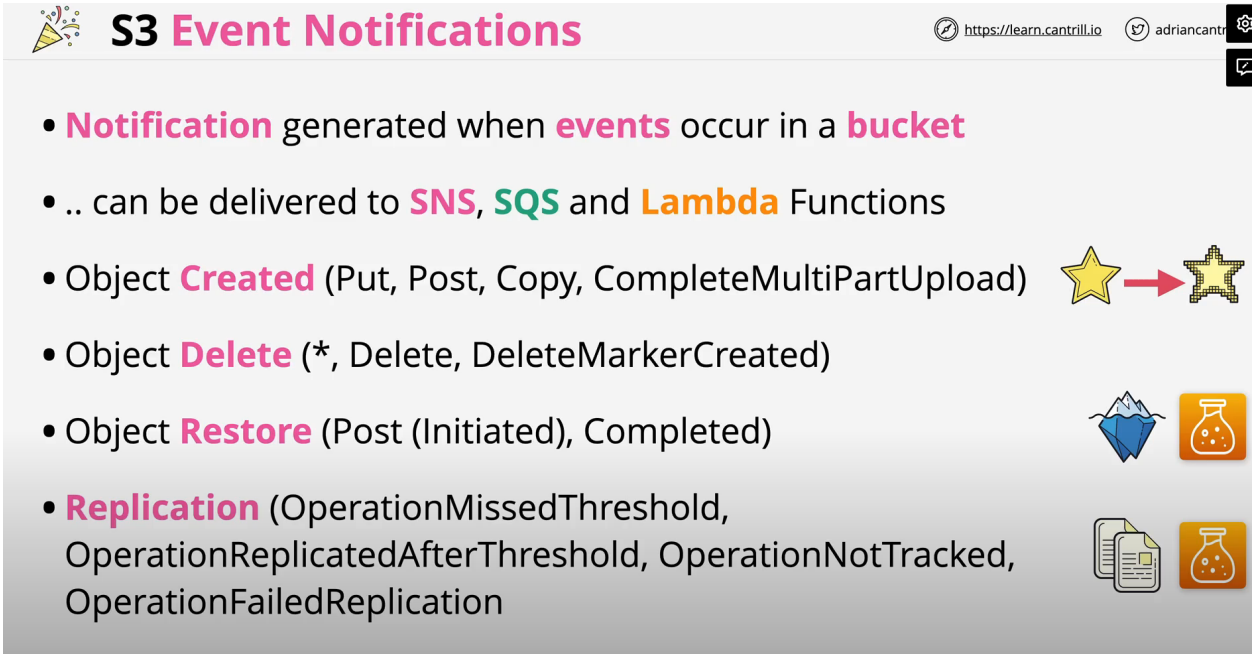
S3 select and Glacier Select

S3 Select and Glacier Select

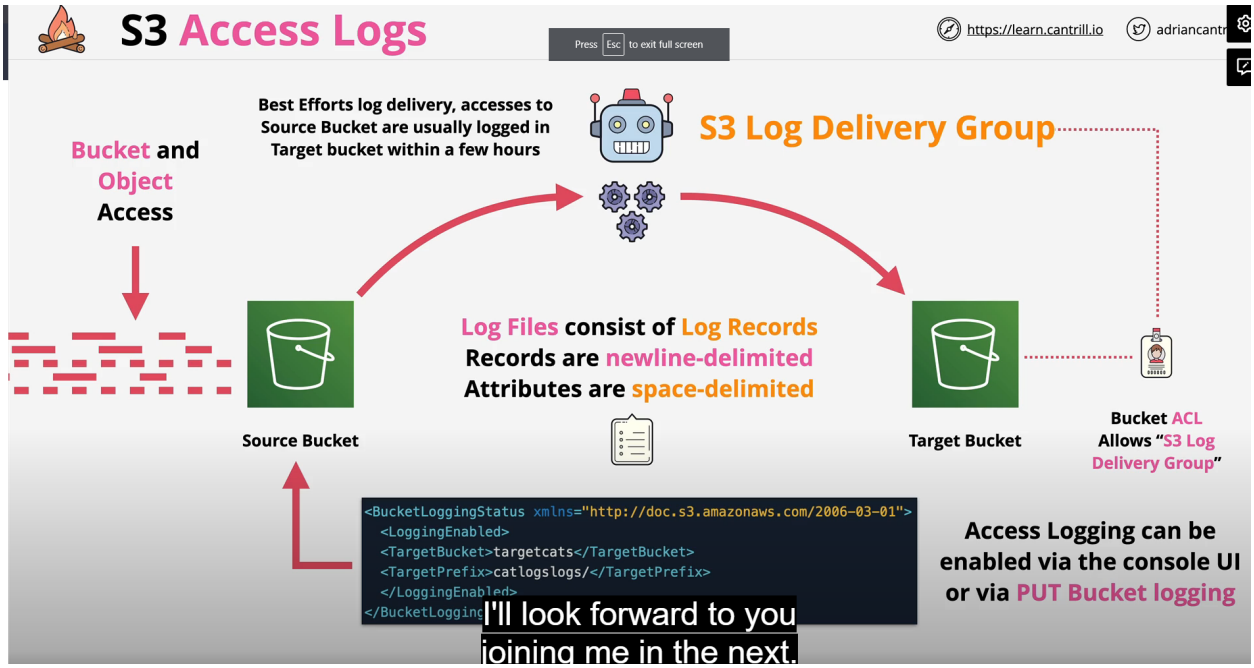
https://learn.cantrill.io adriancantr



S3 EVENT Notification:



S3 Access Logs:


S3 Access Logs
Press Esc to exit full screen
https://learn.cantrill.io
adriancantr
Best Efforts log delivery, accesses to Source Bucket are usually logged in Target bucket within a few hours
S3 Log Delivery Group
Bucket and Object Access
Log Files consist of Log Records
Records are newline-delimited
Attributes are space-delimited
Source Bucket
Target Bucket
Bucket ACL Allows "S3 Log Delivery Group"
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
<LoggingEnabled>
<TargetBucket>targetcats</TargetBucket>
<TargetPrefix>catlogslogs/</TargetPrefix>
</LoggingEnabled>
</BucketLogging
Access Logging can be enabled via the console UI or via PUT Bucket logging
I'll look forward to you joining me in the next.