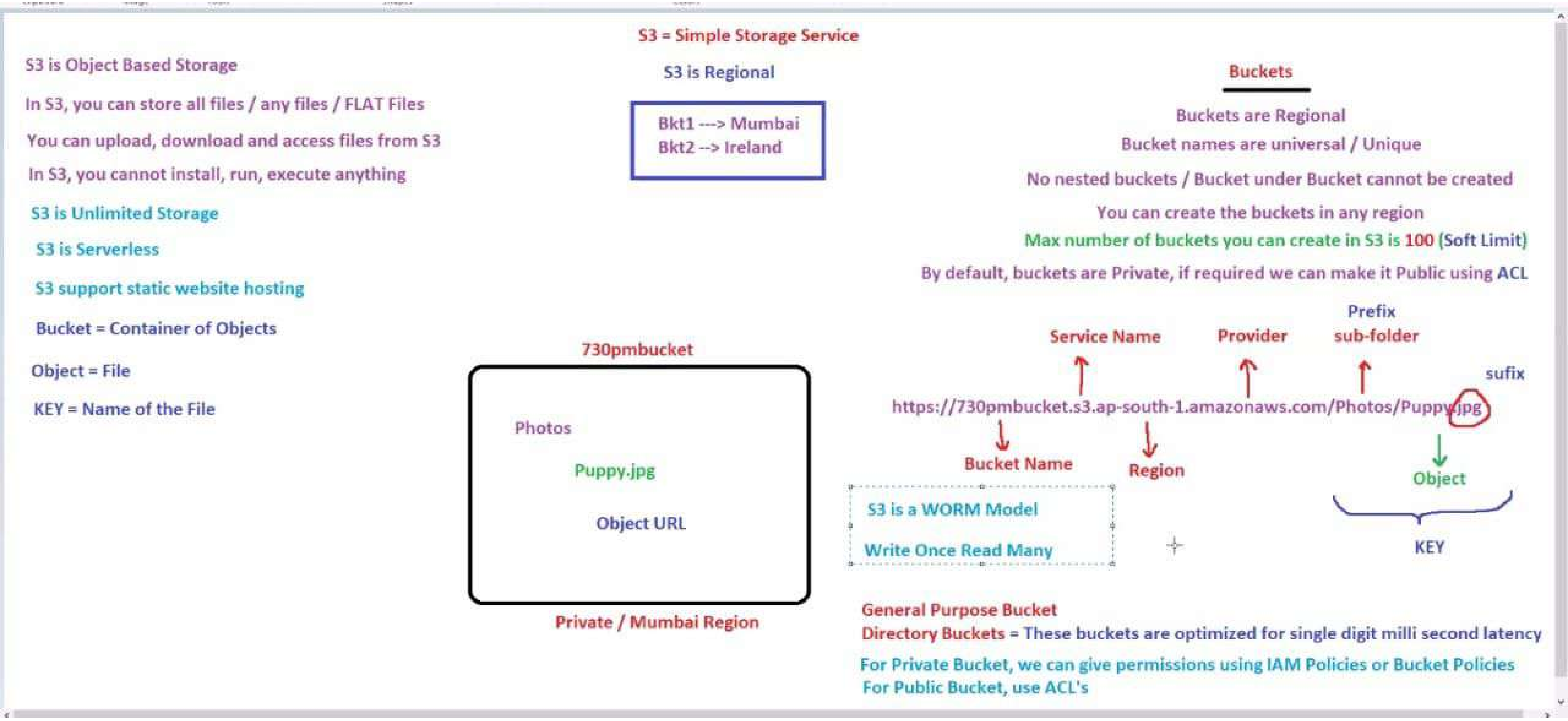


S3 = Simple Storage Service

S3 is Object Based Storage

In S3, you can store all files / any files / FLAT Files

You can upload, download and access files from S3

In S3, you cannot install, run, execute anything

S3 is Unlimited Storage

S3 is Serverless

S3 support static website hosting

Bucket = Container of Objects

Object = File

KEY = Name of the File

S3 is Regional

Bkt1 ---> Mumbai
Bkt2 --> Ireland

730pmbucket

Photos

Puppy.jpg

Object URL

Private / Mumbai Region

Buckets

Buckets are Regional

Bucket names are universal / Unique

No nested buckets / Bucket under Bucket cannot be created

You can create the buckets in any region

Max number of buckets you can create in S3 is 100 (Soft Limit)

By default, buckets are Private, if required we can make it Public using ACL

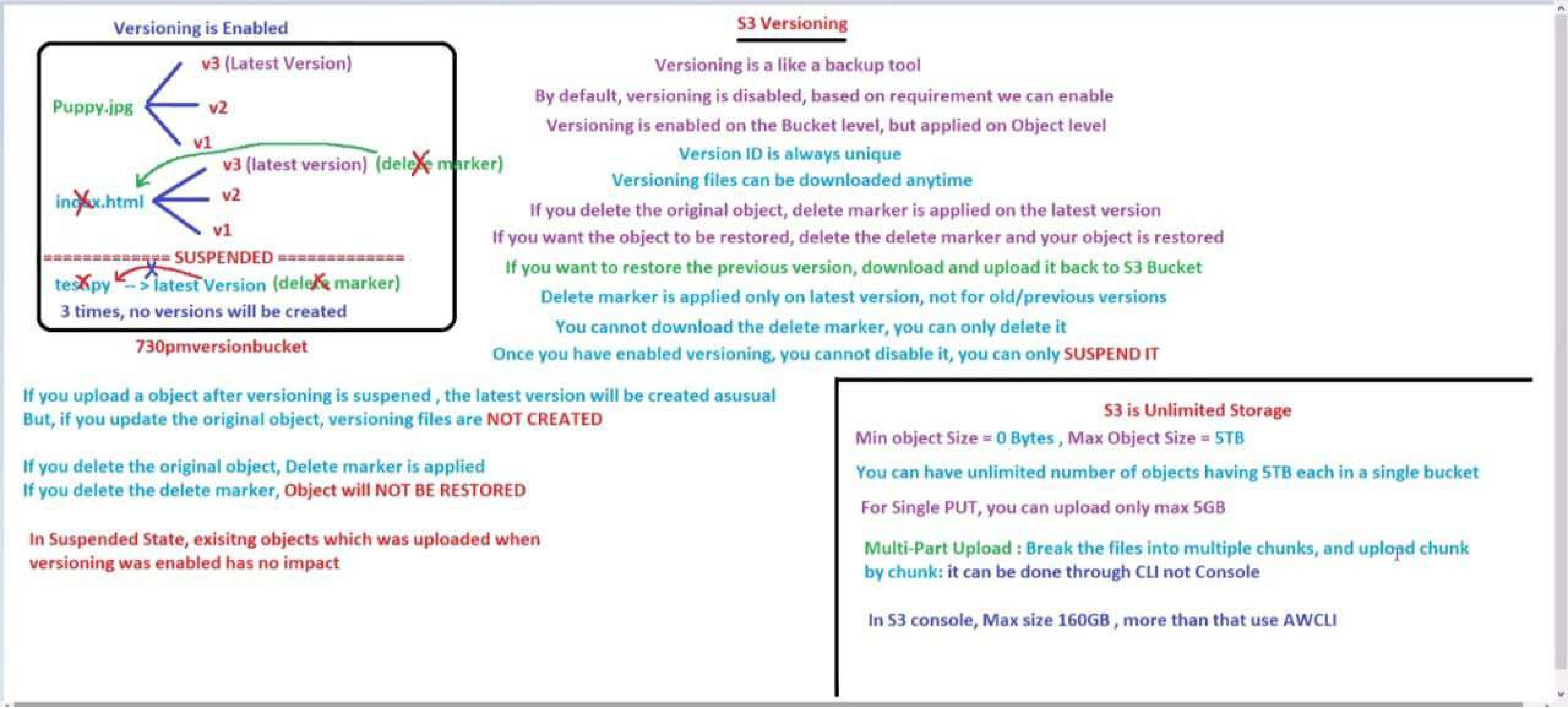
https://730pmbucket.s3.ap-south-1.amazonaws.com/Photos/Puppy.jpg

S3 is a WORM Model

Write Once Read Many

General Purpose Bucket
Directory Buckets = These buckets are optimized for single digit milli second latency

For Private Bucket, we can give permissions using IAM Policies or Bucket Policies
For Public Bucket, use ACL's



Versioning is Enabled

Puppy.jpg
- v3 (Latest Version)
- v2
- v1

index.html
- v3 (latest version) (delete marker)
- v2
- v1

============= SUSPENDED =============

test.py --> latest Version (delete marker)

3 times, no versions will be created

730pmversionbucket

S3 Versioning

Versioning is a like a backup tool

By default, versioning is disabled, based on requirement we can enable

Versioning is enabled on the Bucket level, but applied on Object level

Version ID is always unique

Versioning files can be downloaded anytime

If you delete the original object, delete marker is applied on the latest version

If you want the object to be restored, delete the delete marker and your object is restored

If you want to restore the previous version, download and upload it back to S3 Bucket

Delete marker is applied only on latest version, not for old/previous versions

You cannot download the delete marker, you can only delete it

Once you have enabled versioning, you cannot disable it, you can only SUSPEND IT

If you upload a object after versioning is suspened , the latest version will be created asusual
But, if you update the original object, versioning files are NOT CREATED

If you delete the original object, Delete marker is applied
If you delete the delete marker, Object will NOT BE RESTORED

In Suspended State, exisitng objects which was uploaded when versioning was enabled has no impact

S3 is Unlimited Storage

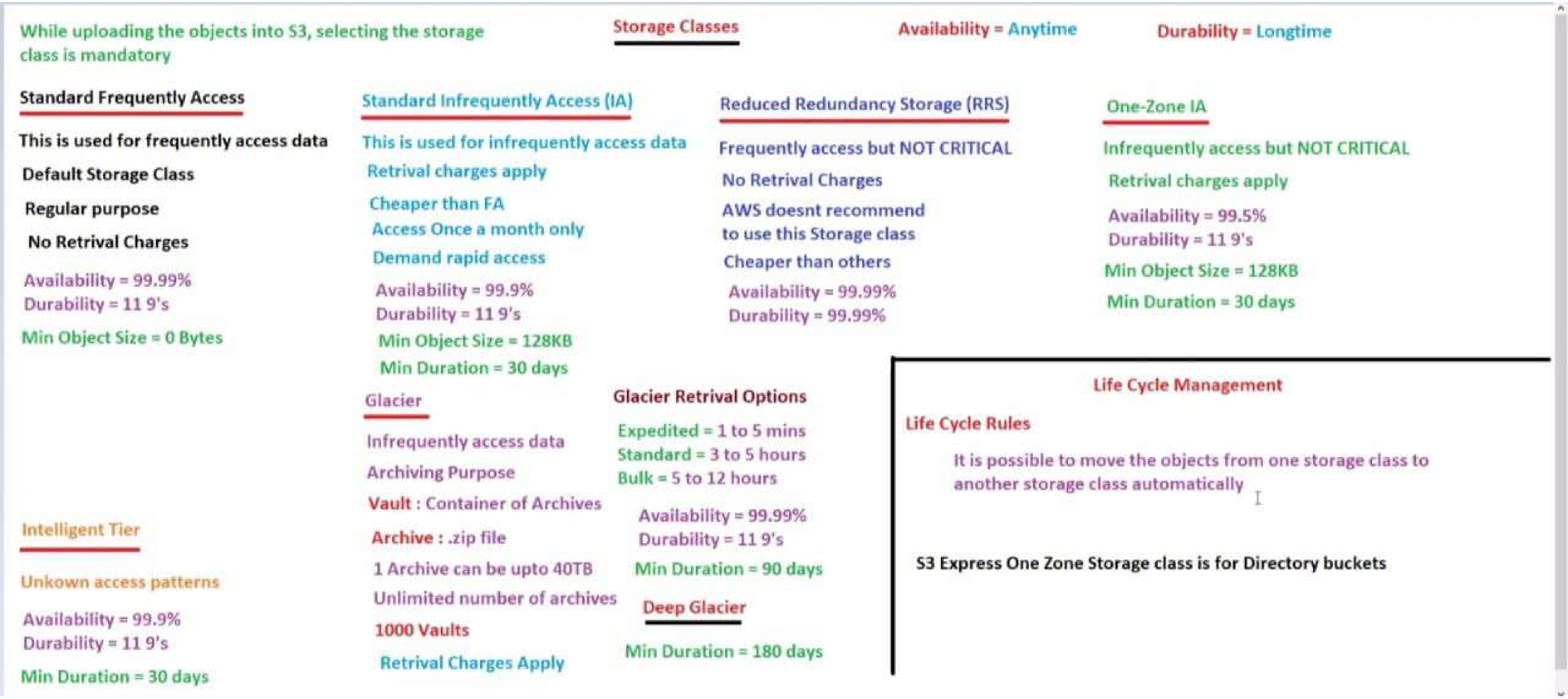
Min object Size = 0 Bytes , Max Object Size = 5TB

You can have unlimited number of objects having 5TB each in a single bucket

For Single PUT, you can upload only max 5GB

Multi-Part Upload : Break the files into multiple chunks, and upload chunk by chunk: it can be done through CLI not Console

In S3 console, Max size 160GB , more than that use AWCLI



Storage Classes

While uploading the objects into S3, selecting the storage class is mandatory

Availability = Anytime

Durability = Longtime

Standard Frequently Access

This is used for frequently access data

Default Storage Class

Regular purpose

No Retrival Charges

Availability = 99.99%
Durability = 11 9's

Min Object Size = 0 Bytes

Intelligent Tier

Unkown access patterns

Availability = 99.9%
Durability = 11 9's

Min Duration = 30 days

Standard Infrequently Access (IA)

This is used for infrequently access data

Retrival charges apply

Cheaper than FA
Access Once a month only

Demand rapid access

Availability = 99.9%
Durability = 11 9's

Min Object Size = 128KB

Min Duration = 30 days

Glacier

Infrequently access data

Archiving Purpose

Vault : Container of Archives

Archive : .zip file

1 Archive can be upto 40TB

Unlimited number of archives

1000 Vaults

Retrival Charges Apply

Reduced Redundancy Storage (RRS)

Frequently access but NOT CRITICAL

No Retrival Charges

AWS doesnt recommend
to use this Storage class

Cheaper than others

Availability = 99.99%
Durability = 99.99%

Glacier Retrival Options

Expedited = 1 to 5 mins
Standard = 3 to 5 hours
Bulk = 5 to 12 hours

Availability = 99.99%
Durability = 11 9's

Min Duration = 90 days

Deep Glacier

Min Duration = 180 days

One-Zone IA

Infrequently access but NOT CRITICAL

Retrival charges apply

Availability = 99.5%
Durability = 11 9's

Min Object Size = 128KB

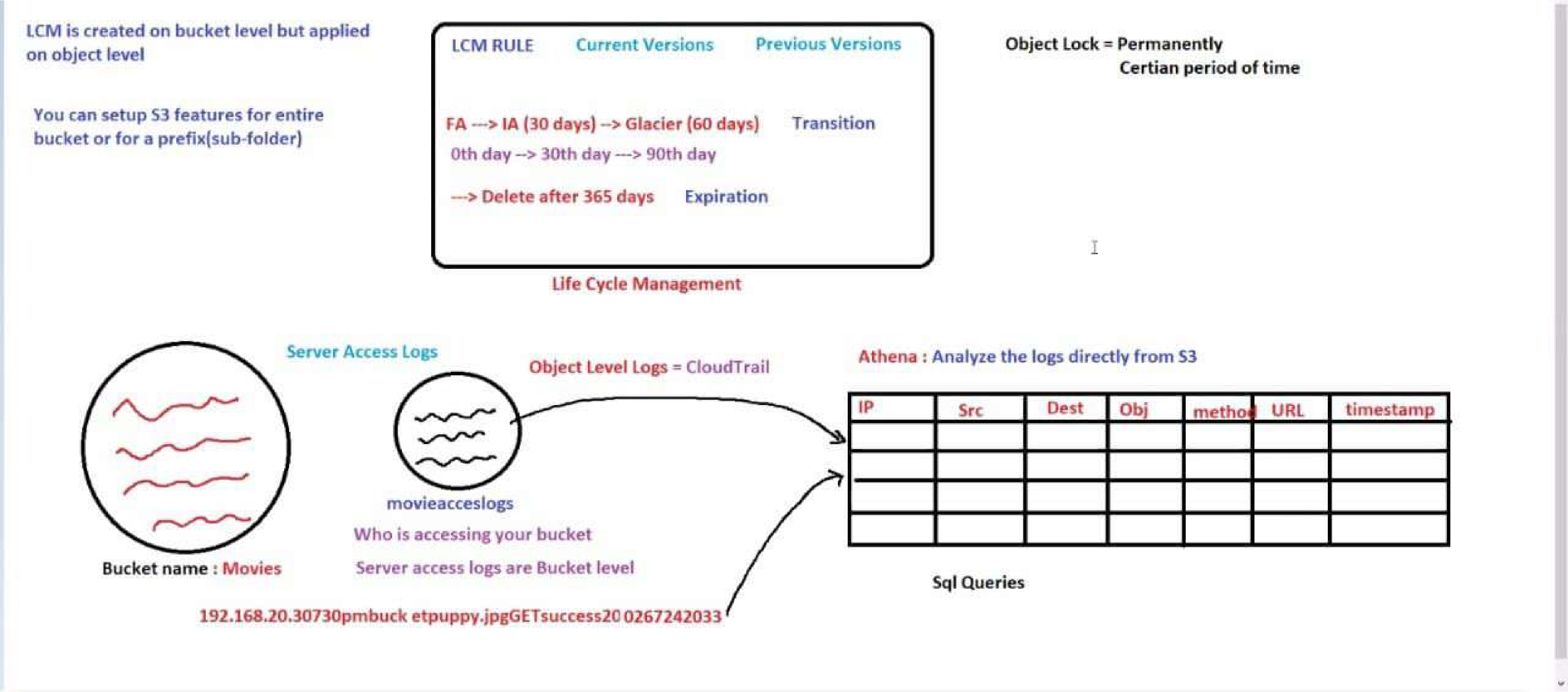
Min Duration = 30 days

Life Cycle Management

Life Cycle Rules

It is possible to move the objects from one storage class to another storage class automatically

S3 Express One Zone Storage class is for Directory buckets



LCM is created on bucket level but applied on object level

You can setup S3 features for entire bucket or for a prefix(sub-folder)

LCM RULE Current Versions Previous Versions

FA ---> IA (30 days) --> Glacier (60 days) Transition

0th day --> 30th day ---> 90th day

---> Delete after 365 days Expiration

Life Cycle Management

Object Lock = Permanently
Certian period of time

Server Access Logs

Bucket name : Movies

movieacceslogs

Who is accessing your bucket

Server access logs are Bucket level

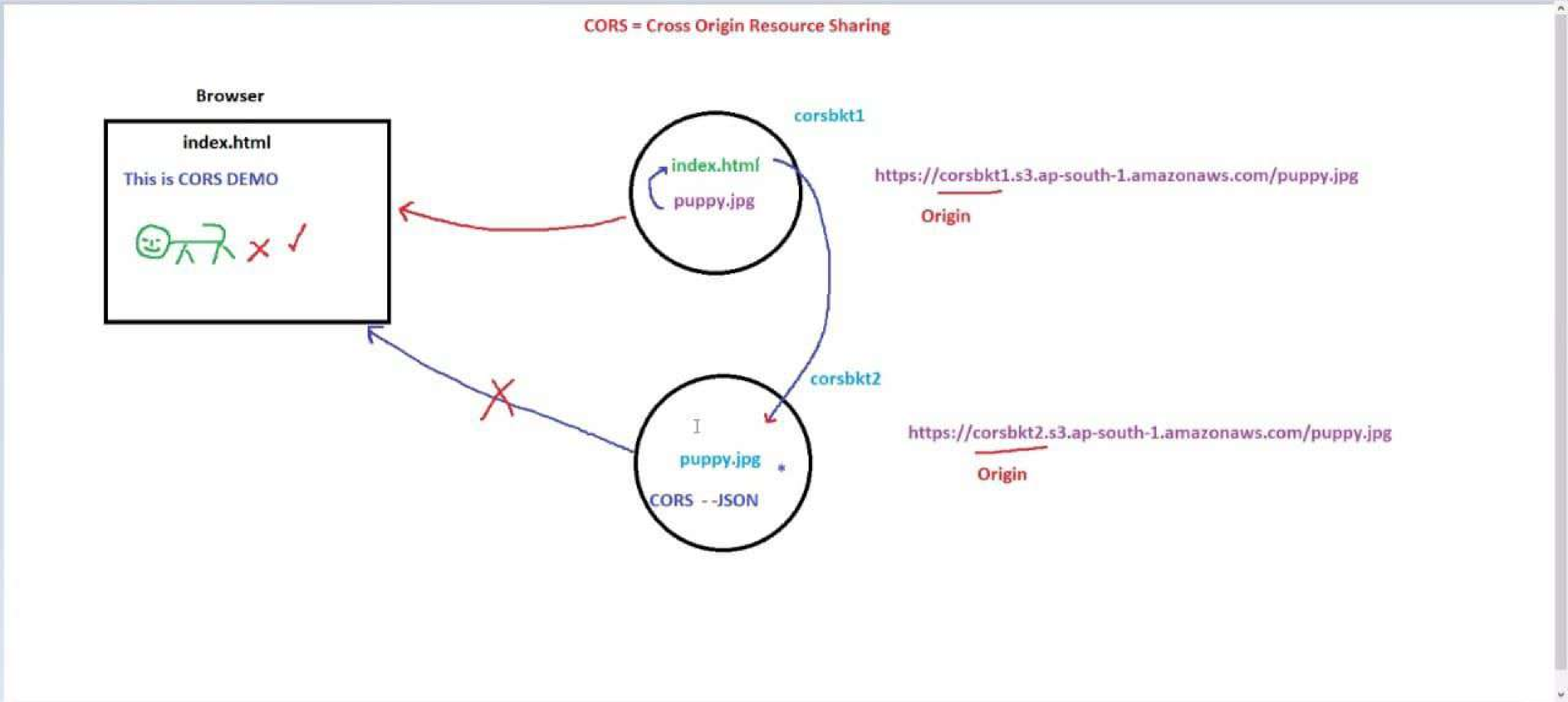
Object Level Logs = CloudTrail

192.168.20.30730pmbuck etpuppy.jpgGETsuccess20 0267242033

Athena : Analyze the logs directly from S3

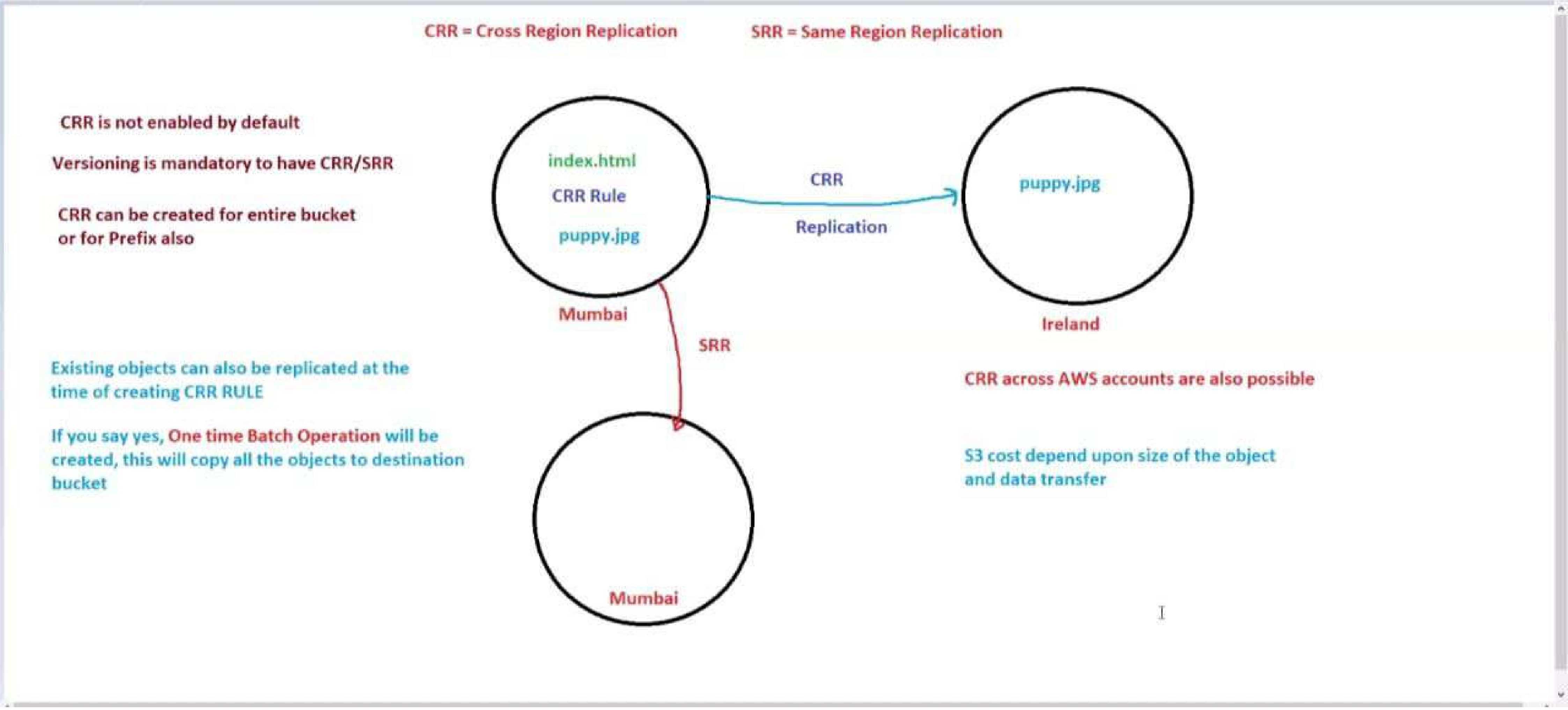
IP	Src	Dest	Obj	method	URL	timestamp

Sql Queries



CORS = Cross Origin Resource Sharing

Browser
index.html
This is CORS DEMO
corsbkt1
index.html
puppy.jpg
https://corsbkt1.s3.ap-south-1.amazonaws.com/puppy.jpg
Origin
corsbkt2
puppy.jpg
CORS - -JSON
https://corsbkt2.s3.ap-south-1.amazonaws.com/puppy.jpg
Origin



CRR = Cross Region Replication

SRR = Same Region Replication

CRR is not enabled by default

Versioning is mandatory to have CRR/SRR

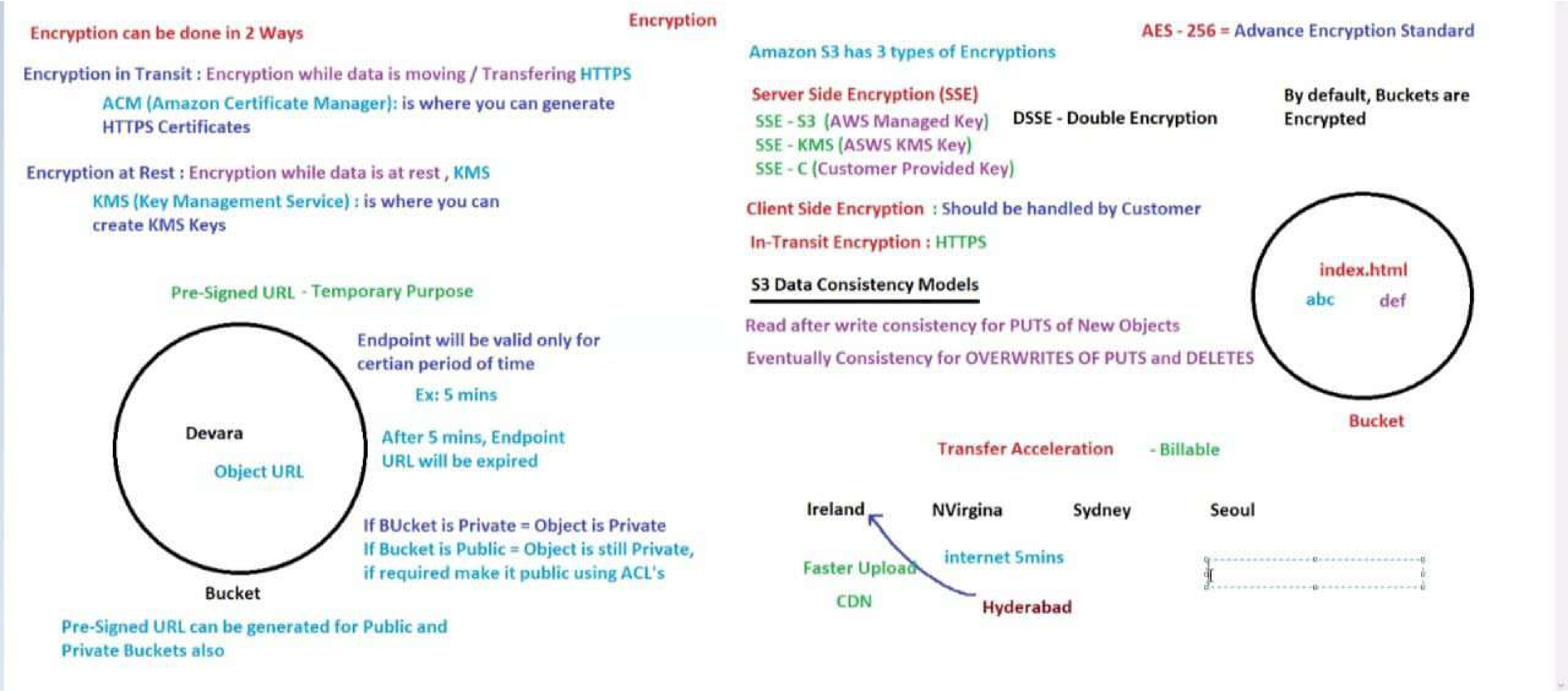
CRR can be created for entire bucket
or for Prefix also

Existing objects can also be replicated at the time of creating CRR RULE

If you say yes, One time Batch Operation will be created, this will copy all the objects to destination bucket

CRR across AWS accounts are also possible

S3 cost depend upon size of the object and data transfer



Encryption

Encryption can be done in 2 Ways

Encryption in Transit : Encryption while data is moving / Transfering HTTPS

ACM (Amazon Certificate Manager): is where you can generate HTTPS Certificates

Encryption at Rest : Encryption while data is at rest , KMS

KMS (Key Management Service) : is where you can create KMS Keys

Pre-Signed URL - Temporary Purpose

Devara

Object URL

Bucket

Endpoint will be valid only for certian period of time

Ex: 5 mins

After 5 mins, Endpoint URL will be expired

If BUcket is Private = Object is Private
If Bucket is Public = Object is still Private, if required make it public using ACL's

Pre-Signed URL can be generated for Public and Private Buckets also

AES - 256 = Advance Encryption Standard

Amazon S3 has 3 types of Encryptions

Server Side Encryption (SSE)

SSE - S3 (AWS Managed Key)
SSE - KMS (ASWS KMS Key)
SSE - C (Customer Provided Key)

DSSE - Double Encryption

By default, Buckets are Encrypted

Client Side Encryption : Should be handled by Customer

In-Transit Encryption : HTTPS

S3 Data Consistency Models

Read after write consistency for PUTS of New Objects

Eventually Consistency for OVERWRITES OF PUTS and DELETES

index.html

abc def

Bucket

Transfer Acceleration - Billable

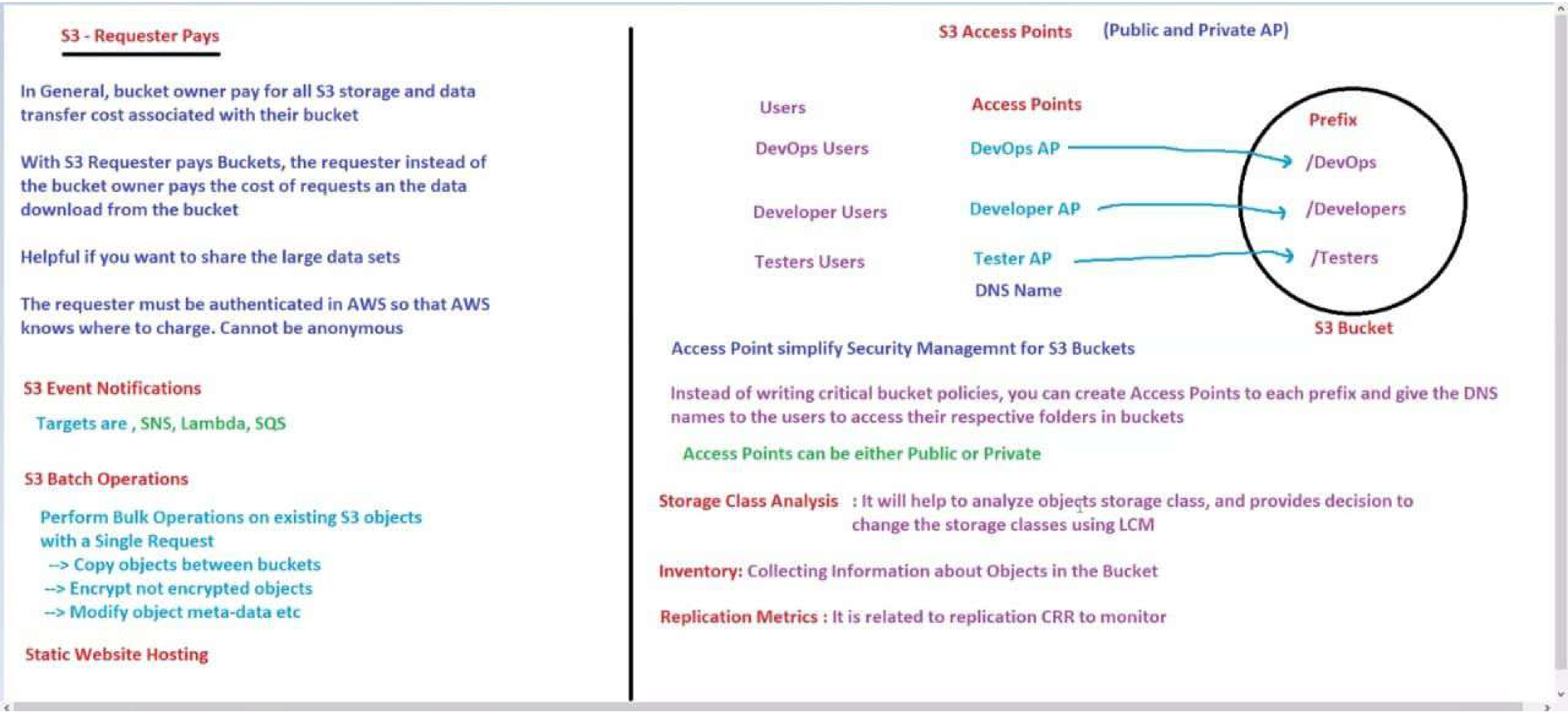
Ireland NVirgina Sydney Seoul

Faster Upload

CDN

internet 5mins

Hyderabad



S3 - Requester Pays

In General, bucket owner pay for all S3 storage and data transfer cost associated with their bucket

With S3 Requester pays Buckets, the requester instead of the bucket owner pays the cost of requests an the data download from the bucket

Helpful if you want to share the large data sets

The requester must be authenticated in AWS so that AWS knows where to charge. Cannot be anonymous

S3 Event Notifications

Targets are , SNS, Lambda, SQS

S3 Batch Operations

Perform Bulk Operations on existing S3 objects with a Single Request

--> Copy objects between buckets
--> Encrypt not encrypted objects
--> Modify object meta-data etc

Static Website Hosting

S3 Access Points (Public and Private AP)

Users
DevOps Users
Developer Users
Testers Users

Access Points
DevOps AP
Developer AP
Tester AP
DNS Name

Prefix
/DevOps
/Developers
/Testers

S3 Bucket

Access Point simplify Security Managemnt for S3 Buckets

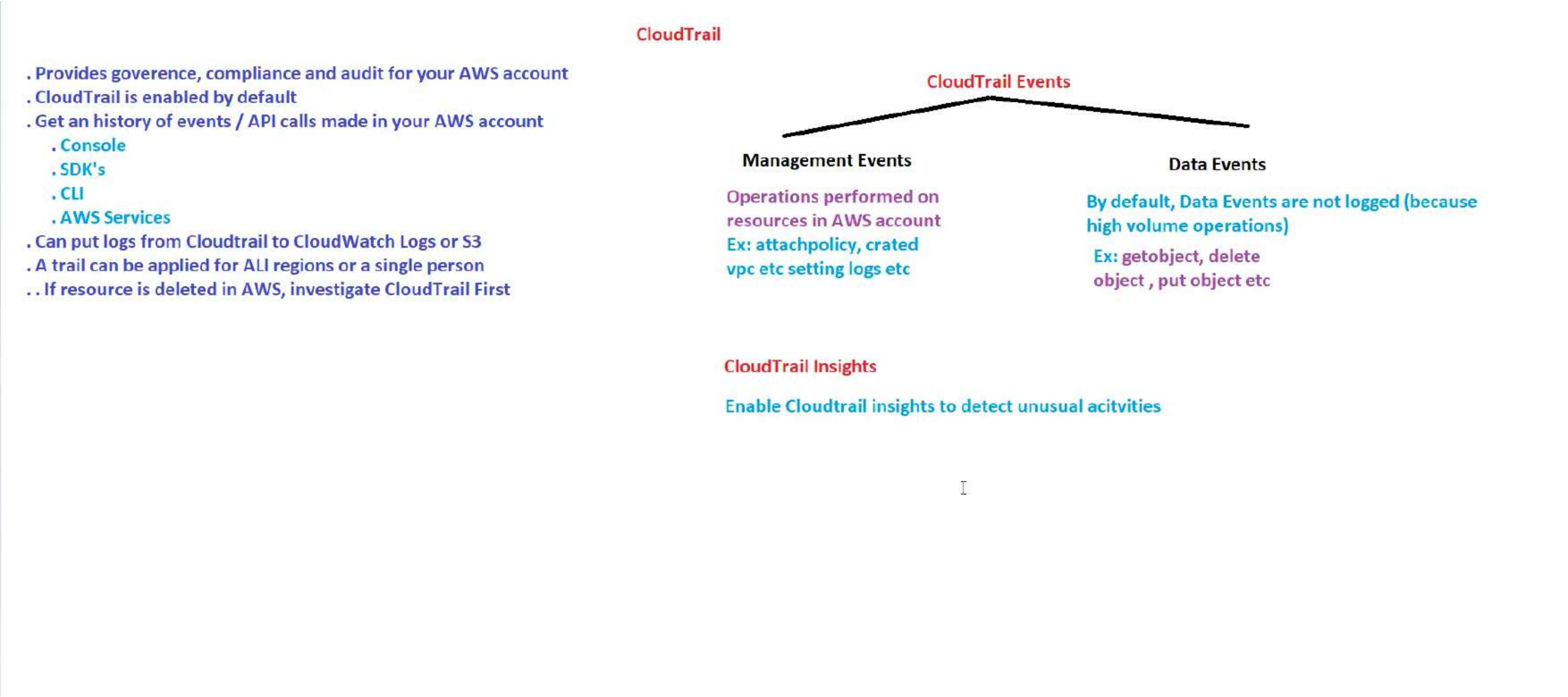
Instead of writing critical bucket policies, you can create Access Points to each prefix and give the DNS names to the users to access their respective folders in buckets

Access Points can be either Public or Private

Storage Class Analysis : It will help to analyze objects storage class, and provides decision to change the storage classes using LCM

Inventory: Collecting Information about Objects in the Bucket

Replication Metrics : It is related to replication CRR to monitor



CloudTrail

- . Provides goverence, compliance and audit for your AWS account
- . CloudTrail is enabled by default
- . Get an history of events / API calls made in your AWS account
  - . Console
  - . SDK's
  - . CLI
  - . AWS Services
- . Can put logs from Cloudtrail to CloudWatch Logs or S3
- . A trail can be applied for ALl regions or a single person
- . . If resource is deleted in AWS, investigate CloudTrail First

CloudTrail Events

Management Events

Operations performed on resources in AWS account

Ex: attachpolicy, crated vpc etc setting logs etc

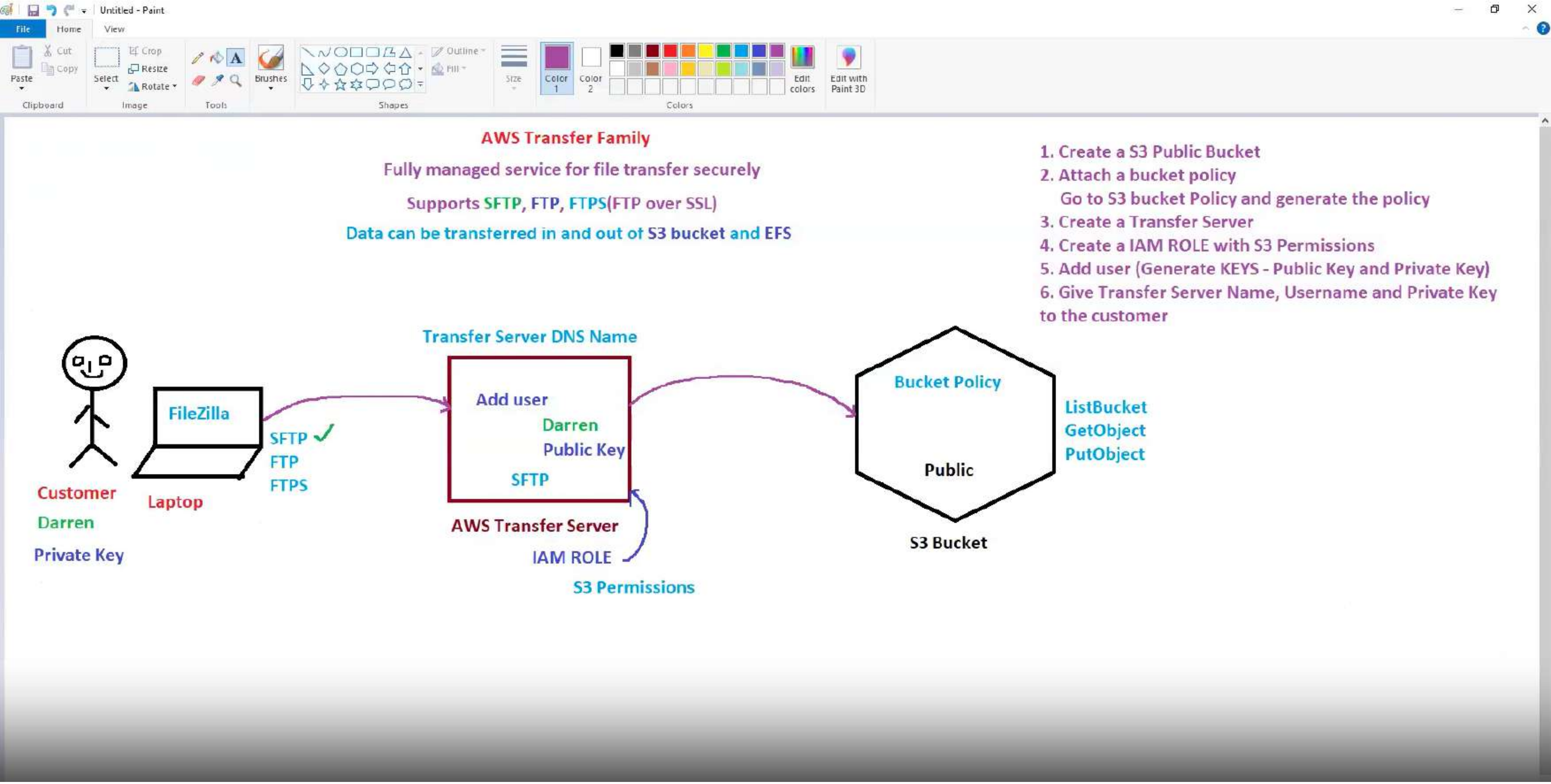
Data Events

By default, Data Events are not logged (because high volume operations)

Ex: getobject, delete object , put object etc

CloudTrail Insights

Enable Cloudtrail insights to detect unusual acitvities



AWS Transfer Family

Fully managed service for file transfer securely

Supports SFTP, FTP, FTPS(FTP over SSL)

Data can be transferred in and out of S3 bucket and EFS

1. Create a S3 Public Bucket
2. Attach a bucket policy
   Go to S3 bucket Policy and generate the policy
3. Create a Transfer Server
4. Create a IAM ROLE with S3 Permissions
5. Add user (Generate KEYS - Public Key and Private Key)
6. Give Transfer Server Name, Username and Private Key to the customer