



S3 Storing objects and Media

- Overview on S3 and
- Security
- Static website hosting and versioning
- Replication and Life cycle configuration
- Event notification
- Demos



@TeamShiksha



@teamShiksha



@teamshiksha



Overview on S3

- S3 allows users to store objects (files) in “buckets” (directories)
- Globally unique name (across all regions all accounts).
- Buckets are defined at the region level.
- Naming convention: No uppercase, No underscore, 3-63 characters long, Not an IP, Must start with lowercase letter or number or **xn--**, must not end with **--s3alias**.

s3://my-bucket/folder1/folder2/my_file.txt

Blue - bucket, red - key (key is composed of prefix + object name(my_file.txt))

- Max. Object Size is 5TB (5000GB)
- Use “multi-part upload” for objects more than 5GB
- Metadata (list of text key / value pairs)
- Tags (key / value pair max 10)
- Version ID (versioning enabled)



@TeamShiksha



@teamShiksha



@teamshiksha



S3 Security

- User-Based
 - IAM Policies - Allowing people to access the bucket or not
- Resource-Based
 - Bucket Policies: Bucket wide rules from the S3 console - allows cross account
- Encryption: encrypt objects in Amazon S3 using encryption keys
- Server-Side Encryption (SSE)
- SSE-KMS, SSE-C(Customer)
- **NOTE:** An IAM can access an S3 object if
 - The user IAM permissions ALLOW it OR the resource policy ALLOWS it and there's no explicit DENY

```
{
  "Version": "2012-10-17",
  "Id": "PutObjPolicy",
  "Statement": [{
    "Sid": "DenyObjectsThatAreNotSSEKMS",
    "Principal": "*",
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
      }
    }
  }]
}
```



@TeamShiksha



@teamShiksha



@teamshiksha



Static website hosting and versioning

- Host static websites and have them accessible on the Internet.
- If you get a 403 Forbidden error, make sure the bucket policy allows public reads
- **Versioning:**
 - You can version your files in S3
 - Enabled at bucket level
 - Sample file name overwrite but creates a version
 - It is best practice to version your buckets
 - Protect against unintended deletes
 - Easy roll back to previous version
 - Notes: File will have `null` version if versioning was not enabled earlier. And versioned file will not be delete if versioning is disabled.



@TeamShiksha



@teamShiksha



@teamshiksha



S3 Storage Classes

<https://aws.amazon.com/s3/storage-classes/>

	Standard	Intelligent-Tiering	Standard-IA	One Zone-IA	Glacier Instant Retrieval	Glacier Flexible Retrieval	Glacier Deep Archive
Durability	99.999999999% == (11 9's)						
Availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.9%	99.9%
Availability Zones	>= 3	>= 3	>= 3	1	>= 3	>= 3	>= 3
Min. Storage Duration Charge	None	None	30 Days	30 Days	90 Days	90 Days	180 Days
Min. Billable Object Size	None	None	128 KB	128 KB	128 KB	40 KB	40 KB
Retrieval Fee	None	None	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved





Replication and Life cycle

Replication

- Must enable Versioning in source and destination buckets (Cross-region and Same-region replication). Buckets can be of different AWS accounts
- Process is asynchronous and you must give proper permissions
- Only new objects are replicated (S3 Batch Replication for replicating existing objects)
- Can replicate delete markers from source to target (optional setting)
- There should not be “chaining” of replication (A -> B -> C, Object won't replicate on C)

Lifecycle Rules

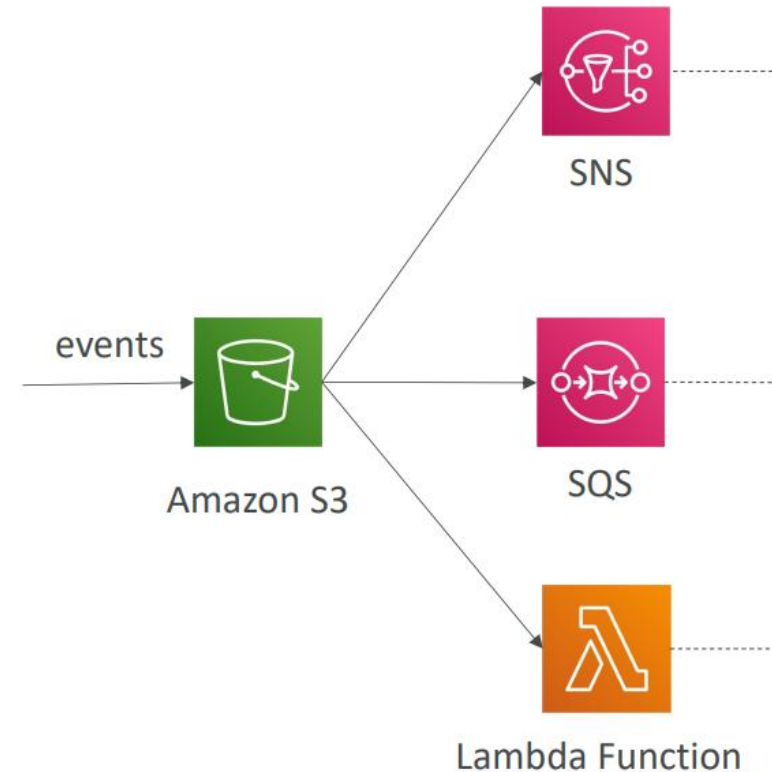
- Object life cycle is automation required for your transition between storage classes. (For archive objects that you don't need fast access to, move them to Glacier or Glacier Deep Archive.)
- **Transition Actions** - configure objects to transition to another storage class
- **Expiration actions** - configure objects to expire (delete) after some time
- Rules can be created for a certain prefix or tags





Even notification

- S3:ObjectCreated, S3:ObjectRemoved, S3:ObjectRestore, S3:Replication
- Object name filtering possible
- Can create as many “S3 events” as desired
- S3 event notifications typically deliver events in seconds but can sometimes take a minute or longer
- Use case: generate thumbnails of images uploaded to S3
- Advanced filtering options with JSON rules
- Multiple Destinations
- EventBridge Capabilities



@TeamShiksha



@teamShiksha



@teamshiksha