

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 an 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 turned 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

- 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 S3 does not provide client-side encryption.
- 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 a bucket in another AWS Account
- Transfer Acceleration provides faster and secure uploads from anywhere in the world. Data is uploaded via a distinct URL to an Edge Location. Data is then transported to your S3 bucket via AWS backbone network.
- Presigned URIs is a URL generated via the AWS CLI and SDK. It provides temporary access to write or download object data. Presigned URIs are commonly used to access private objects.

S3 has 6 different Storage Classes:

1. Standard Fast! 99.99% Availability, 11 9's Durability. Replicated across at least three AZs
2. 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.
3. 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)

4. S3 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.
5. S3 Glacier For long-term cold storage. Retrieval of data can take minutes to hours but the off is very cheap storage
6. S3 Glacier Deep Archive The lowest cost storage class. Data retrieval time is 12 hours.