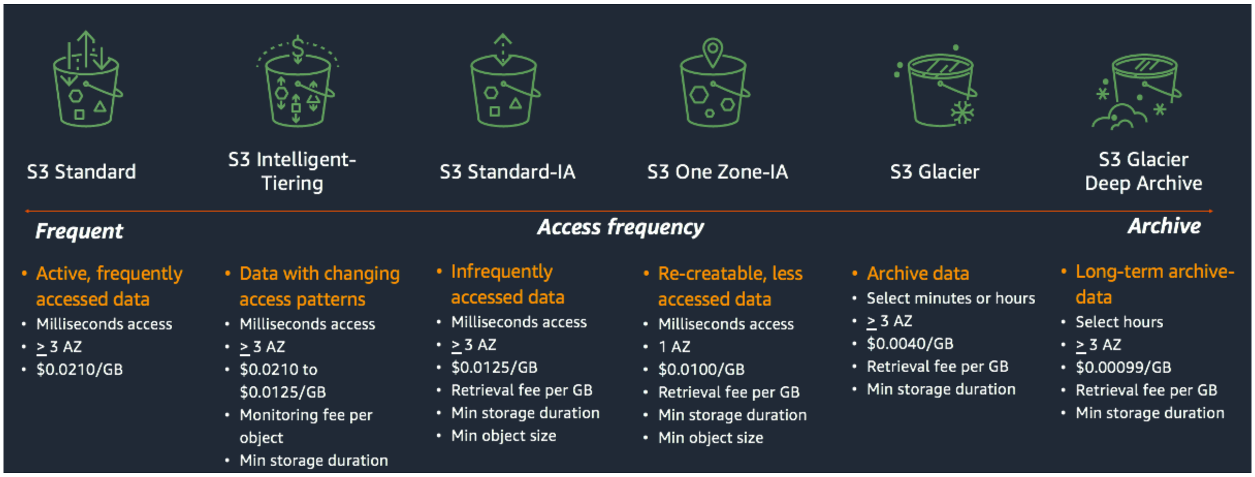
Module 3 – S3

S3 Bucket

Allows you to store and retrieve data on the internet. It's designed to provide a highly scalable, durable, and secure solution for object storage. The only condition for creating the S3 bucket is the name should be unique.

S3 storage classes.



Frequent — Access frequency — Archive

S3 Standard	S3 Intelligent-Tiering	S3 Standard-IA	S3 One Zone-IA	S3 Glacier	S3 Glacier Deep Archive
• Active, frequently accessed data • Milliseconds access • ≥ 3 AZ • $0.0210/GB	• Data with changing access patterns • Milliseconds access • ≥ 3 AZ • $0.0210 to $0.0125/GB • Monitoring fee per object • Min storage duration	• Infrequently accessed data • Milliseconds access • ≥ 3 AZ • $0.0125/GB • Retrieval fee per GB • Min storage duration • Min object size	• Re-creatable, less accessed data • Milliseconds access • 1 AZ • $0.0100/GB • Retrieval fee per GB • Min storage duration • Min object size	• Archive data • Select minutes or hours • ≥ 3 AZ • $0.0040/GB • Retrieval fee per GB • Min storage duration	• Long-term archive-data • Select hours • ≥ 3 AZ • $0.00099/GB • Retrieval fee per GB • Min storage duration

How to Create S3 Bucket.

- Search for S3 services and click on Create Bucket.
- Specify in which AWS region we want this bucket to be created.
- Bucket type General Purpose and provide the unique name for the bucket.
- Enabled ACL and Public access. Rest keeps the default setting.

S3 Bucket Properties

1. **Versioning**, should it continue to be disabled by default?
   Enabling versioning for your Amazon S3 bucket can be **good practice** in many scenarios.
   - ***Accidental Deletions***: With versioning enabled, every object in your bucket will have multiple versions. This can protect you from accidental deletions or overwrites, as older versions of objects are preserved.
   - ***Data Recovery***: Versioning provides a way to recover previous versions of objects that might have been modified or deleted by mistake.
   - *Data Auditing*: Versioning can assist in auditing changes to objects. You can track who made changes and when they were made.
   - ***Legal and Compliance Requirements***: Some industries or regulations require data retention and audit trails. Versioning can help meet these requirements.

- ***Collaboration and Collaboration*:** If multiple people or processes are accessing and modifying objects in the bucket, versioning can help manage conflicts and changes more effectively.
- ***Rollback to Previous States***: If you need to revert to a previous version of an object, versioning simplifies this process.

2. Should **logging** be enabled by default?

   Logging should always be enabled when multiple users access the resource and as good practice.

   - You can record the actions that are taken by *users*, *roles*, or *AWS services* on Amazon S3 resources and maintain log records for auditing and compliance purposes. AWS recommends, using *server-access logging*, *AWS CloudTrail logging*, or a combination of both. We are in final stages of implementing a log server and If the logs are delivered to us, we can have them processed by our own server.
   - Logs are never deleted from AWS, only archived.

3. Is S3 Bucket **logging disabled** by **default**?
   - Yes. They require you to enable and choose logs from a source bucket of your choice.
4. Where should the logs be stored by default?
   - AWS by Default
5. What should be logged by default?
   - It depends on what you are needing to review. Below is a list of the default logged items.

   Each access log record provides details about, a single access request such as:

   - *The requester,*
   - *bucket name,*
   - *request time,*
   - *request action,*
   - *response status, and error code (if any).*
   - *Access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill.*
6. Should we disable http (allow only https) by default?
   - Some apps might use http as a starting point and do a redirect like Outlook365. Maybe adding a redirection would be more beneficial.
7. S3 Bucket Replication is disabled. Should bucket replication be enabled?
   - For redundancy, I would recommend enabling this feature.
8. When is this ever enabled by default?
   - By **default**, all S3 objects are private, so S3 needs permissions to replicate objects from a source bucket.
9. S3 Bucket SSL policy (deny old SSL protocols below TLS 1.2). This seems like a good policy to have in place.
   - It's best practice to use modern encryption protocols for data in transit.

   Note: Customers must use TLS version 1.2 or later to access content that's stored in your S3 buckets.
10. S3 Bucket MFA is disabled, how do we reconcile MFA for automated FTP jobs?
    - You'll need to use temporary security credentials in combination with MFA. Below is quick view of what is needed:
      - IAM Role
      - MFA Device
      - Temporary Security Credentials
11. S3 Bucket not encrypted with KMS, what does this even mean?

- Key Management Service – In context of Amazon is a service that provides centralized management of the encryption keys used to encrypt your S3 data.

12. How would this be implemented?

    To encrypt an Amazon S3 bucket with AWS Key Management Service (KMS), you can follow these general steps:

    - Create a KMS Key: Log in to your AWS Management Console, go to the KMS service, and create a new customer managed key. Take note of the key ID.
    - Update Bucket Policy: In your S3 bucket, update the bucket policy to allow the KMS key to access objects. You'll need to add an appropriate "kms:Decrypt" permission using the KMS key's ARN in the bucket policy.
    - Choose Encryption Setting: In the S3 bucket properties, under "Default encryption", select the option to enable default encryption using the KMS key you created.
    - Update Object ACLs (Optional): You can also set object-level permissions using the KMS key. This adds an extra layer of control on top of the bucket policy.

Static Web Site hosting on S3 bucket

- Follow the steps of creating the S3 bucket.

index.html

- Upload the attached Index.html page to the bucket.
- Click on Properties and in the bottom get the URL to browse.