STORAGE
IN
AWS

S3

Amazon Simple Storage Service (Amazon S3) is a scalable, high-speed, web-based cloud storage service designed to store and retrieve any amount of data at any time. It uses an object storage architecture, where data is managed as objects rather than file hierarchies.

Each object in S3 is stored in a bucket and consists of data, metadata, and a unique identifier. S3's key features include high (99.999999%) durability, availability, security, and performance. It's widely used for backup and recovery,content distribution, static website hosting, etc, making it a fundamental service for many cloud-based applications.

It is also the cheapest of the three major forms of storage in AWS, the others being: Block Storage using EBS (Elastic Block Store), which is used in databases and File Storage using EFS.

The cost for the three services is as follows:

S3 ⇒ Cheapest (i.e. Least expensive)

EFS ⇒ Cheaper

EBS ⇒ Least Cheap

EFS and Multiple Access

Amazon Elastic File System (EFS) is a scalable, fully managed, POSIX-compatible file storage service .

EFS is highly available and durable, making it ideal for workloads that require shared access to file storage across multiple instances. It does cost more than S3 but less than EBS (Elastic Block Store).

It also has a Infrequent Access (EFS-IA) feature which functions similar to S3-IA though its lifecycle policies with regards to IA are much more limited than its S3 counterpart.

EBS and Fast Snapshot Restore

Amazon Elastic Block Store (EBS) is a high-performance block storage service designed for use with EC2 instances. It provides persistent block-level storage volumes that can be attached to EC2 instances, allowing you to store data and access it from any instance. EBS volumes are durable and highly available, offering features such as snapshots for data backup and replication for data protection.

Note:

EBS has a feature called Fast Snapshot Restore which can be used to clone data from an EC2 instance store into new EBS volumes with minimal time, reducing the amount of required to recover or create new volumes.

Provisioned IOPS

Provisioned IOPS (PIOPS) is a storage option offered by AWS for applications requiring high-performance and consistent input/output operations per second (IOPS).

It is designed for use with Amazon EBS (Elastic Block Store) and is ideal for I/O-intensive applications such as large databases, transactional systems, and other performance-sensitive workloads especially when compared to General Purpose SSD.

AWS DataSync

AWS DataSync is a service provided by Amazon Web Services (AWS) that simplifies, accelerates, and automates the process of transferring data between on-premises storage systems and AWS services.

After the initial migration, AWS DataSync can be configured to maintain the consistency of data between on-premises storage and AWS storage services.

Data Synchronization also happens in near real-time.

While both AWS DataSync and AWS Storage Gateway provide solutions for integrating on-premises storage environments with AWS cloud storage services, they serve different purposes and have distinct functionalities, including how they handle data synchronization:

1. **AWS DataSync**:
    - **Purpose**: Primarily designed for high-speed, one-time data transfers and ongoing data synchronization between on-premises storage systems and AWS storage services.
    - **Data Transfer Mechanism**: Utilizes optimized data transfer protocols to ensure fast and efficient transfer of large volumes of data.
    - **Use Cases**: Ideal for scenarios requiring frequent updates or synchronization of data between on-premises and AWS environments, such as continuous data backup, real-time data processing, or maintaining consistent copies of data for disaster recovery purposes.
2. **AWS Storage Gateway**:
    - **Purpose**: Offers a hybrid storage solution that enables on-premises applications to seamlessly access data stored in AWS cloud storage

services.

- **Data Synchronization**: While AWS Storage Gateway supports data migration and synchronization capabilities, its primary focus is on providing on-demand access to data stored in AWS, rather than continuous synchronization.
- **Storage Protocols**: Supports various storage protocols, including NFS, SMB, and iSCSI, allowing existing on-premises applications to interact with AWS storage as if it were local storage.
- **Use Cases**: Commonly used for extending on-premises storage capacities, disaster recovery, data archiving, and enabling cloud-based applications to access on-premises data.

Data transfer times

Transferring large amount of data into AWS

- Example: transfer 200 TB of data in the cloud. We have a 100 Mbps internet connection.
- Over the internet / Site-to-Site VPN:
  - Immediate to setup
  - Will take 200(TB)*1000(GB)*1000(MB)*8(Mb)/100 Mbps = 16,000,000s = 185d
- Over direct connect 1Gbps:
  - Long for the one-time setup (over a month)
  - Will take 200(TB)*1000(GB)*8(Gb)/1 Gbps = 1,600,000s = 18.5d
- Over Snowball:
  - Will take 2 to 3 snowballs in parallel
  - Takes about 1 week for the end-to-end transfer
  - Can be combined with DMS
- For on-going replication / transfers: Site-to-Site VPN or DX with DMS or DataSync

Snowmobile Capacity

AWS Snowmobile is a secure data transport service designed for transferring extremely large amounts of data (up to 100 petabytes) to AWS.

Snowmobile is ideal for large-scale migrations such as data center shutdowns, archives, and content libraries, offering a fast and cost-effective way to transfer massive datasets to the cloud securely.

Snowball Edge vs Snowball

AWS Snowball is a data migration service that uses secure, ruggedized devices to transfer large amounts of data into and out of AWS. It simplifies and accelerates data migration, reducing the challenges of network bandwidth limitations.

AWS Snowball Edge extends this functionality by adding computing capabilities. It comes with built-in storage and compute power, enabling local data processing and analysis before transferring data to AWS.

Basically, AWS Snowball Edge can run EC2 Instances and lambda functions, allowing for Edge Computing Instances which the normal Snowball cannot. You do pay a little extra for this privilege, however.

Specifications for Snowball and Snowball Edge:

Snowball: 50 to 80 TB

Snowball Edge: 80TB HDD to 210TB Nvme

S3 File Gateway

S3 File Gateway is a hybrid cloud storage solution that seamlessly integrates on-premises applications with Amazon S3. It presents S3 buckets as NFS or SMB file shares, allowing applications to access objects stored in S3 using familiar file protocols.

Note:

Because of the hybrid nature of the service, S3 File Gateway can be used to give low-latency access to data if and when needed.

FSX for Lustre

As the name says, FSX for Lustre is designed for Linux and/or Lustre workloads, if the question asks to design architecture for HPC, it is FSX for Lustre.

FSX for Windows

FSx for Windows File Server is a fully managed file storage service built on Windows Server, providing highly reliable and scalable file storage that is accessible over the Server Message Block (SMB) protocol.

FSx for Windows File Server eliminates the complexity of managing and maintaining traditional file servers, offering automatic backups, continuous monitoring, and integration with AWS services. It is designed to support Windows applications that require shared file storage, such as Microsoft SQL Server, SAP, and home directories for users.

FSX for windows also has a File Gateway that works similarly to S3 File Gateways.

Compliance vs Governance Object Lock

Object Lock is a feature of Amazon S3 that helps enforce compliance by preventing deletion or modification of objects for a specified retention period. It ensures that data remains immutable and protected against accidental or malicious deletion, supporting regulatory requirements and data governance policies.

The two types of Object Lock in Amazon S3 are:

1. **Retention Periods**: This mode sets a fixed retention period during which objects cannot be deleted or altered. It ensures data immutability for compliance with regulations like SEC Rule 17a-4(f) and the General Data Protection Regulation (GDPR).
2. **Legal Hold**: This mode allows you to place legal holds on objects, which prevents them from being deleted by any user until the hold is removed. It is typically used for preserving data relevant to legal or investigative proceedings.

Also, object lock has two modes namely:

Compliance Object Lock ⇒ Stuff cannot be changed, even by governing authorities.

Governance Object Lock ⇒ Stuff can be changed by governing authorities.

Legal Hold vs Retention Periods

Legal Hold vs. Retention Period

With Object Lock, you can also place a legal hold on an object version. Like a retention period, a legal hold prevents an object version from being overwritten or deleted. However, a legal hold doesn't have an associated retention period and remains in effect until removed. Legal holds can be freely placed and removed by any user who has the **s3:PutObjectLegalHold** permission.

Legal holds are independent from retention periods.

Object lock enforces WORM.

S3 Bucket Policy VS IAM Policy

S3 bucket policies and IAM policies are both crucial for managing access control in AWS, but they serve different purposes and scopes.

S3 Bucket Policies: These are attached directly to S3 buckets and define permissions for all objects within the bucket. Bucket policies are written in JSON and can specify access permissions based on IP address, AWS account, or other conditions.

IAM Policies: These are attached to IAM identities (users, groups, roles) and specify what actions they can perform on AWS resources and are also written in JSON but are more granular, allowing fine-tuned control over specific AWS services and resources. They define permissions based on actions, resources, and conditions.

Basically, S3 bucket policies control access to S3 buckets and their contents based on conditions like IP address or AWS account, while IAM policies control access related to actions, resources, and identities within an AWS account.

S3 Intelligent Tiering

One of the various different storage classes available for S3. S3 Intelligent tiering moves data between S3 Standard and S3 IA as it sees fit. With S3 standard being the default base S3 storage class and S3 IA (Infrequent Access) being designed for data that requires immediate access but is not accessed frequently.

S3 Intelligent Tiering utilizes proprietary algorithms to determine which objects are to be kept in the standard class and which objects are to be moved to S3 IA.

S3 Intelligent tiering is used in cases where some files are accessed frequently while other files are rarely accessed in an unpredictable pattern.

S3 Glacier Deep Archive

The Amazon S3 Glacier storage classes offer purpose-built solutions for cost-effective , data archival storage. They provide virtually unlimited scalability and ensure 99.999999999% (11 nines) data durability.

These classes include options for rapid access to archived data and economical cloud storage solution.].Users can select from three archive storage classes optimized for various access patterns and storage durations.

For immediate access needs, such as medical images or genomics data, the S3 Glacier Instant Retrieval storage class provides low-cost storage with millisecond retrieval times.

For scenarios requiring occasional large-scale data retrieval at minimal cost, such as backup or disaster recovery, the S3 Glacier Flexible Retrieval (formerly S3 Glacier) offers retrieval times in minutes or free bulk retrievals within 5-12 hours.

Lastly, for cost-effective, long-term storage like compliance archives or digital media preservation, users can opt for S3 Glacier Deep Archive, which provides very low-cost storage with data retrieval within twelve hours.

Athena

Amazon Athena is a serverless, interactive query service that allows you to analyze data directly in Amazon S3 using standard SQL. It eliminates the need for complex ETL processes and infrastructure setup, enabling you to start querying data immediately. With Athena, you pay only for the queries you run, making it a cost-effective solution for ad-hoc data analysis and reporting.

Basically,

Amazon Athena can be used to run queries on-demand on an S3 bucket.

(Even in JSON format)

Transfer Acceleration

Amazon S3 Transfer Acceleration speeds up file transfers to and from Amazon S3 by using AWS's globally distributed edge locations. It leverages Amazon CloudFront's network of edge locations to route data optimally, reducing latency and improving upload and download speeds, especially for users far from the S3 bucket's region. This service is ideal for transferring large files or data sets quickly and efficiently.

Quick Tip: Aggregate the data from all these global sites as quickly as possible in a single Amazon S3 bucket ⇒ S3 Transfer Acceleration

Accidental Deletion

To prevent accidental deletion of your data in AWS, it is **very important** to use **Versioning** and **Multi-Factor Authentication (MFA)**.

Versioning keeps multiple versions of an object in an S3 bucket, allowing you to recover previous versions if an object is mistakenly deleted or overwritten.

MFA Delete adds an extra layer of security by requiring additional authentication for delete operations, ensuring that only authorized users can permanently remove data. Implementing these features helps safeguard your critical data against accidental or unauthorized deletion.