AWS S3

AWS S3 (Simple Storage Service) is a highly durable and scalable object storage service offered by Amazon Web Services (AWS). It allows users to store and retrieve large amounts of data, such as files, images, videos, and more, in a secure and reliable manner.

- **Working of S3**

  Key Components

1. Buckets: S3 stores data in buckets, which are essentially containers that hold objects. Buckets are the top-level namespace for S3, and they can be thought of as a folder in a file system.

2. Objects: Objects are the individual files stored in S3. Each object has a unique key (also known as a key-value pair) that consists of a name and a value. The name is the object's key, and the value is the object's contents.

3. Regions: S3 is a distributed system with multiple regions around the world. Each region has multiple Availability Zones (AZs), which are isolated locations within a region that are designed to be highly available and fault-tolerant.

4. Nodes: S3 nodes are the individual servers that store and serve objects. Each node is responsible for a portion of the overall S3 storage capacity.

1. Object Ownership

The **"Bucket Owner Enforced"** setting in **Amazon S3 Object Ownership** ensures that **the bucket owner automatically owns all objects** stored in the bucket, **regardless of who uploads them**. This setting **disables Access Control Lists (ACLs)**, enforcing a unified access policy using **IAM policies and bucket policies** instead.

2. Block Public Access settings for this bucket

The **Block Public Access** settings in Amazon S3 **prevent unauthorized public access** to your bucket and objects. This feature helps **protect sensitive data** by ensuring that no one can accidentally expose your files to the internet.

3. **Bucket policy**

A **Bucket Policy** in Amazon S3 is a JSON-based access control policy that defines permissions for **who can access the bucket and its objects**. It provides **fine-grained control** over access by specifying **which actions** are allowed or denied for **specific AWS accounts, IAM users, or public access**.

Cloud Front

1. Origin Access

Public – Allows anyone on the internet to access the S3 bucket directly. (**Not recommended** for security reasons.)

Origin Access Control Settings (Recommended) – Uses **Origin Access Control (OAC)** to restrict access to the S3 bucket, ensuring only CloudFront can retrieve content. This is the **new recommended method**.

Legacy Access Identities (**Selected in the image**) – Uses an **Origin Access Identity (OAI)** to grant CloudFront permission to access the S3 bucket while keeping it private from the public.

2. Bucket Policy Update

No, I will update the bucket policy – Requires the user to manually update the S3 bucket policy to allow CloudFront access.

Yes, update the bucket policy (**Selected in the image**) – Automatically updates the S3 bucket policy to allow CloudFront to read objects via the OAI. This is the **easiest and recommended option** to ensure proper access permissions.

3. Viewers

- **HTTP and HTTPS** – Allows both HTTP and HTTPS connections.
  - **Least secure** because HTTP is unencrypted.
  - Useful for backward compatibility, but **not recommended** for sensitive data.
- **Redirect HTTP to HTTPS** (**Selected in the image**)
  - If a user requests content over **HTTP**, CloudFront **automatically redirects** them to **HTTPS**.
  - **Recommended** because it ensures **secure connections** while still allowing HTTP requests.
- **HTTPS Only**
  - Rejects all HTTP requests and allows only **HTTPS connections**.
  - Provides **maximum security** but may block users if they try to access using HTTP.

4. Web Application Firewall (WAF)

1️⃣ Enable Security Protections

- Activates AWS WAF for this CloudFront distribution.
- Filters incoming traffic and blocks **malicious requests** before they reach your web servers.
- Helps protect against **common web threats** and improves security.

2️⃣ Do Not Enable Security Protections (**Selected in the image**)

- No WAF protection is applied to this CloudFront distribution.
- CloudFront will **not** filter incoming requests, leaving the application more exposed to attacks.