**Task: Enable Server Access Logging in S3**

**Name:** Abhishek Hengade

**Batch:** B-56

This document provides a comprehensive guide on how to enable server access logging for an Amazon S3 bucket. This feature is crucial for security audits, monitoring access patterns, and understanding traffic to your bucket.

**## 1. Understanding Server Access Logging**

Server access logging provides detailed records for all requests made to your S3 bucket. When enabled, S3 captures comprehensive log data for actions like GET, PUT, and DELETE on objects. These logs are then delivered as text files to a designated target S3 bucket.

**## 2. Important Best Practice: Use a Separate Bucket for Logs**

Before you begin, it is critical to understand that the **destination bucket for your logs must be different from the source bucket you are monitoring.**

If you set the destination to be the same as the source, you will create an infinite logging loop:

1. A user accesses a file in your bucket.
2. S3 writes a log file about that access *to the same bucket*.
3. This "write" action is itself a request that needs to be logged.
4. S3 then writes another log file about the log file it just wrote, and this process repeats indefinitely, rapidly increasing your storage costs.

Therefore, the first step is always to create a new, separate S3 bucket dedicated solely to receiving logs.

**## 3. Step-by-Step Guide to Enabling Server Access Logging**

* **Step 1: Navigate to Bucket Properties** From the S3 console, select the bucket you wish to monitor (the source bucket). In this case, yoga-bucket. Click on the **Properties** tab and scroll down to the **Server access logging** section.
* **Step 2: Edit Logging Configuration** Click the **Edit** button. On the "Edit server access logging" page, select **Enable**.
* **Step 3: Specify the Destination for Logs** This is the most critical step. Under **Destination**, you must specify the separate S3 bucket you created for logging.
  + **Target bucket**: Click **Browse S3** and select your dedicated logging bucket (e.g., yoga-bucket-logs).
  + **Target prefix**: It is highly recommended to specify a prefix (like logs/ or yoga-bucket-logs/). This organizes all log files into a folder within the destination bucket, making them much easier to manage.
* **Step 4: Save and Verify** Click **Save changes**. S3 will automatically update the target bucket's policy to grant the S3 logging service the necessary permissions to deliver log files. A success banner will appear, and the server access logging status will now show as **Enabled**, pointing to your chosen destination bucket.

