**Task Description**

Create an S3 bucket, with no public access and upload files to the bucket & view the logs using CloudWatch for the uploaded files.

**Step 1: Create an S3 Bucket**

* Navigate to S3 in AWS Management Console.
* Create the Bucket - Click **"Create Bucket"**

A screenshot of a computer

Description automatically generated

* Enter a unique **Bucket Name** (myguvitaskbucket).
* **Bucket Type:**  General Purpose
* **Object Ownership:** ACLs disabled

A screenshot of a computer

Description automatically generated

* Ensure **Block Public Access** is enabled (default setting).
* Optionally enable **Bucket Versioning** and **Encryption**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Click **"Create Bucket"**.

**A screenshot of a computer

Description automatically generated**

**Step 2: Enable Logging for the S3 Bucket**

* Go to your bucket's Properties tab.

**A screenshot of a computer

Description automatically generated**

* Enable Server Access Logging and specify a destination bucket for logs.

A screenshot of a computer

Description automatically generated

* Set permissions for the log destination bucket to allow logging from your source bucket.

A screenshot of a computer

Description automatically generated

**Step 3: Upload Files to the S3 Bucket**

* Go to the Objects tab in your S3 bucket.

A screenshot of a computer

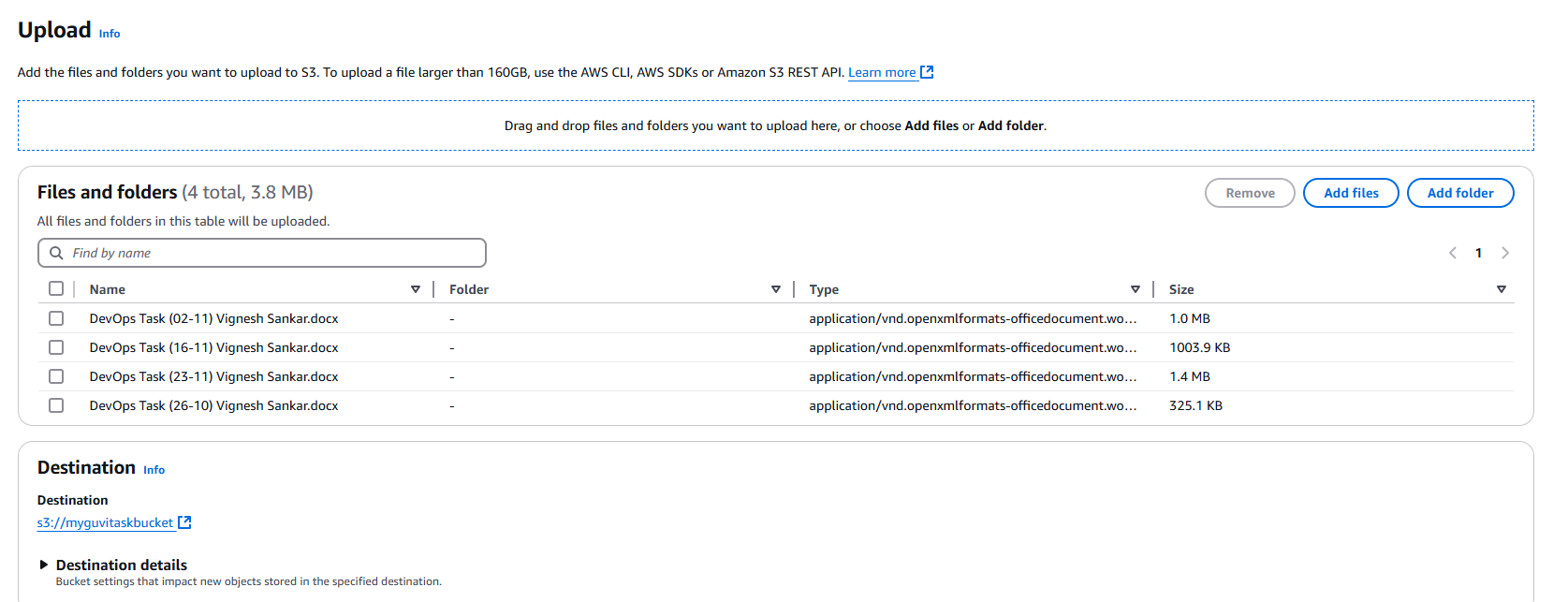
Description automatically generated

* Click "Upload", then select the files you want to upload.

A screenshot of a computer

Description automatically generated

* Review and upload.



**Step 4: Configure CloudWatch for Logs**

* Set Up Event Notifications - go to the **Properties** tab.

A screenshot of a computer

Description automatically generated

* Scroll down to the **Event notifications** section.
* Click **"Create event notification"**

A screenshot of a computer

Description automatically generated

* **Name**: Give it a name (e.g., UploadEvents).
* **Event Types**: Choose **PutObject** (triggered when a file is uploaded to the bucket).

A screenshot of a computer

Description automatically generated

* **Destination**: Select **Amazon EventBridge**.

**Step 5: Enable CloudTrail for Detailed S3 Access Logs in CloudWatch**

* Create Trail

A screenshot of a computer

Description automatically generated

* Enter a **Trail name** (S3AccessTrail)

A screenshot of a computer

Description automatically generated

**Enable CloudWatch Logs:**

* Under the CloudWatch Logs section, select Enable.
* Choose an existing log group or create a new one (e.g., /aws/s3/access-logs).
* Attach a role with permissions for CloudTrail to write to CloudWatch**.**

**A screenshot of a computer

Description automatically generated**

**Enable S3 Data Events**:

* Scroll down to the **Storage location** section.
* Select **S3** under **Management events** and **Data events**.
* Choose **All S3 buckets** or a specific bucket for monitoring.
* Select PutObject, GetObject, and other relevant actions.

A screenshot of a computer

Description automatically generated

* Successfully created Trails

A screenshot of a computer

Description automatically generated