

# Assignment: Configuring a Static Website using AWS S3 & Route 53 and Storing Website Logs

## Objective

The goal of this assignment is to understand how to use AWS S3 to host a static website, use Route 53 for domain name management, and configure S3 to store access logs for the website.

## Requirements

- An AWS account with appropriate permissions to create and manage S3 buckets and Route 53 hosted zones.
- A registered domain name (you can use a domain registered with any domain registrar or register a new domain via Route 53).

## Tasks

### Task 1: Set Up an S3 Bucket for Static Website Hosting

1. **Log in to the AWS Management Console.**
2. **Create an S3 Bucket:**
  - Go to the S3 service in the AWS Management Console.
  - Click on "Create bucket".
  - Enter a globally unique name for your bucket (e.g., `my-static-website-bucket`).

- Choose the region where you want to create the bucket.
- Uncheck "Block all public access" to allow public access to the bucket (necessary for website hosting).
- Acknowledge that the bucket will be public.
- Click "Create bucket".

### **3. Enable Static Website Hosting:**

- Click on the bucket name to open the bucket.
- Go to the "Properties" tab.
- Scroll down to "Static website hosting" and click "Edit".
- Select "Enable" and choose "Host a static website".
- Enter `index.html` as the index document.
- Enter `error.html` as the error document (if you have one).
- Click "Save changes".

### **4. Upload Website Files to S3:**

- Go to the "Objects" tab in your bucket.
- Click "Upload" and add the files for your static website (e.g., `index.html`, `error.html`, and other assets like CSS, JavaScript, images).
- Click "Upload".

### **5. Make the Files Public:**

- Select the uploaded files (e.g., `index.html`).
- Click "Actions" and choose "Make public".
- Confirm to make the files public.

## **Task 2: Configure Route 53 to Route Traffic to the S3 Bucket**

### **1. Register a Domain (if not already registered):**

- Go to the Route 53 service in the AWS Management Console.

- Click on "Registered Domains" and then "Register Domain".
- Follow the steps to register a new domain.

## 2. Create a Hosted Zone:

- In the Route 53 console, click on "Hosted zones".
- Click "Create hosted zone".
- Enter your domain name (e.g., `example.com`).
- Choose "Public hosted zone".
- Click "Create hosted zone".

## 3. Create an S3 Bucket Policy for Website Access:

- Go back to the S3 service and select your bucket.
- Go to the "Permissions" tab.
- Click on "Bucket policy" and add the following policy (replace `my-static-website-bucket` with your bucket name):

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::my-static-website-bucket/*"
```

```
}  
]  
}
```

### 1. Configure DNS Settings in Route 53:

- In the Route 53 console, click on your hosted zone.
- Click "Create record".
- Select "Simple routing" and click "Next".
- Choose "A - IPv4 address" for the record type.
- For the value, select "Alias to S3 website endpoint".
- Select the region and the S3 bucket endpoint corresponding to your bucket.
- Click "Define simple record" and then "Create records".

### Task 3: Set Up S3 Bucket for Access Logs

#### 1. Create a New S3 Bucket for Logs:

- Go to the S3 service in the AWS Management Console.
- Click on "Create bucket".
- Enter a unique name for the bucket (e.g., `my-website-logs-bucket`).
- Choose the region and configure the bucket settings as needed.
- Click "Create bucket".

#### 2. Enable Logging on the Website S3 Bucket:

- Go to the S3 service and select your website bucket (e.g., `my-static-website-bucket`).
- Go to the "Properties" tab.
- Scroll down to "Server access logging" and click "Edit".

- Select "Enable" and choose the target bucket for logs (e.g., `my-website-logs-bucket`).
- Optionally, specify a log prefix (e.g., `logs/`).
- Click "Save changes".

### 3. Set Permissions for Logging:

- Ensure that the logs bucket policy allows the website bucket to write logs.
- Go to the "Permissions" tab of the logs bucket (e.g., `my-website-logs-bucket`).
- Click on "Bucket policy" and add the following policy (replace `my-static-website-bucket` with your bucket name and `my-website-logs-bucket` with your logs bucket name):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-website-logs-bucket/logs/*",
      "Condition": {
        "StringEquals": {
```

```
"s3:x-amz-acl": "bucket-owner-full-control"
    }
  }
}
]
}
```

#### Task 4: Test the Configuration

##### 1. Access the Website:

- Open a web browser and go to your domain (e.g., <http://example.com>).
- Verify that your static website is loading correctly.

##### 2. Generate Website Traffic:

- Visit various pages of your website to generate access logs.

##### 3. Check Logs in S3:

- Go to the S3 service and open your logs bucket (e.g., [my-website-logs-bucket](#)).
- Verify that log files are being created in the specified prefix (e.g., [logs/](#)).

##### 4. Troubleshoot if Necessary:

- Ensure that the S3 bucket policy allows public access.
- Verify that the files in the S3 bucket are public.
- Check the Route 53 DNS settings and ensure they point to the correct S3 website endpoint.

- Ensure the S3 bucket name matches the domain name if using a root domain (e.g., `example.com` bucket for `example.com` domain).
- Ensure the logging configuration is correct and that the logs bucket policy allows writes from the website bucket.

### **Deliverables**

1. **A report** detailing the steps followed for each task, including:
  - Screenshots of the S3 bucket configuration.
  - Screenshots of the Route 53 DNS settings.
  - Screenshots of the logs stored in the S3 logs bucket.
  - URL of the hosted static website.
2. **Description of any issues** encountered and how they were resolved.