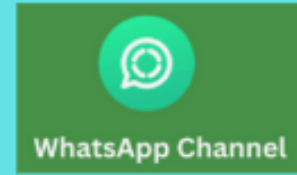


@devopschallengehub



# Various Scenario based questions on S3:part2

## ◆ 6. Describe a scenario where you used S3 as a static website host.

- Uploaded HTML/CSS/JS files to S3 ✓
- Enabled "**Static website hosting**" in bucket properties ✓
- Set up **index.html** and **error.html** documents ✓
- Made bucket public or used **CloudFront** for secure access ✓
- Configured **Route 53** for custom domain routing ✓
- Set up **SSL/TLS certificates** with AWS Certificate Manager ✓
- Implemented **cache control headers** for performance optimization ✓

## ◆ 7. How would you automate backup from S3 to another S3 bucket or Glacier?

- Use **S3 Cross-Region Replication (CRR)** or **Same-Region Replication (SRR)** ✓
- Configure **lifecycle rules** to transition objects to Glacier based on age ✓
- Use **AWS Backup** or **Lambda functions** for custom backup logic ✓
- Set up appropriate **IAM roles and permissions** ✓
- Implement **versioning** on source and destination buckets ✓
- Consider **S3 Batch Operations** for existing objects ✓
- Monitor the replication status with **S3 replication metrics** ✓

## ◆ 8. Suppose you accidentally made your S3 bucket public. How would you fix it immediately?

- Enable (not disable) "**Block Public Access**" settings at both account and bucket levels ✓
- Remove any **public bucket policy** or **object ACLs** ✓
- Use **AWS Config/CloudWatch/GuardDuty** to detect and alert on public buckets ✓
- Review **CloudTrail logs** to assess potential exposure ✓
- Use **S3 Access Analyzer** to identify and remediate unintended access ✓

## ◆ 9. How can you track access to your S3 buckets for auditing purposes?

- Enable **S3 Server Access Logging** to log access requests ✓
- Use **AWS CloudTrail** to track API calls ✓
- Enable **CloudWatch Metrics/Alarms** for unusual activity ✓
- Implement **S3 Event Notifications** for specific actions ✓
- Use **AWS Athena** to query and analyze logs ✓
- Configure **AWS Config** rules to monitor compliance ✓

✓ **Answer: A. AWS CloudTrail**

### ✓ **Sample CloudTrail Event (JSON format)**

```
json
CopyEdit
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAEXAMPLEID1234",
    "arn": "arn:aws:iam::123456789012:user/john.doe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAEXAMPLEKEY",
    "userName": "john.doe"
  },
  "eventTime": "2025-05-19T10:33:21Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.45",
  "userAgent": "aws-cli/2.4.10 Python/3.9.7",
  "requestParameters": {
    "bucketName": "my-s3-bucket",
    "key": "uploads/image1.jpg"
  },
  "responseElements": {
    "x-amz-request-id": "EFGH123456789XYZ",
    "x-amz-id-2": "abc123xyz456def789ghi"
  },
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "AuthenticationMethod": "AuthHeader",
    "vpceEndpointId": "vpce-0a1b2c3d4e5f67890"
  },
  "requestID": "EFGH123456789XYZ",
  "eventID": "abcd1234-5678-90ef-gh12-ijklmnop3456",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "123456789012"
}
```

---

## What you can learn from this:

Field	Meaning
eventName	API call made (PutObject)
userIdentity.userName	Who made the request (john.doe)
sourceIPAddress	IP of the caller
requestParameters.bucketName	Bucket name (my-s3-bucket)
requestParameters.key	Object key uploaded (uploads/image1.jpg)
eventTime	Time of the API call
userAgent	Tool used to make the call (e.g., AWS CLI)

---

## Use Cases:

- **Audit activity** in your AWS account
- **Investigate security incidents**
- **Track changes** to resources (e.g., who deleted or uploaded files)
- Feed into **SIEM tools or Amazon CloudWatch** for alerts

## Example of an S3 Server Access Log entry:

swift

CopyEdit

```
79a5fEXAMPLE my-bucket [19/May/2025:10:35:22 +0000] 192.0.2.3 - 3A4VEXAMPLE
REST.GET.OBJECT photos/cat.jpg "GET /photos/cat.jpg HTTP/1.1" 200 - 1234 678 10 9 "-"
"Mozilla/5.0" -
```



## Breakdown of key fields in the log entry:

Field	Description
79a5fEXAMPLE	Requester's Canonical User ID
my-bucket	Name of the bucket
[19/May/2025:10:35:22 +0000]	Date and time of the request
192.0.2.3	IP address of the requester
3A4VEXAMPLE	Request ID
REST.GET.OBJECT	Operation (GET Object in this case)
photos/cat.jpg	Key of the object accessed
"GET /photos/cat.jpg HTTP/1.1"	HTTP Request Line
200	HTTP status code
1234	Size of the object in bytes

Mozilla/5.0	User-Agent string (browser or tool used)
-------------	--

### Why use Server Access Logs:

- Track **who accessed which objects** and when.
- Monitor **unauthorized access** attempts.
- Analyze **data usage patterns**.
- Help with **auditing and security reviews**.

### Why use both cloud trail for s3 and S3 Server Access Logs?

Aspect	CloudTrail for S3	S3 Server Access Logs
Tracks API calls	✅ (Who called which API)	❌ (Does not show API calls or users)
Tracks HTTP requests	❌ (Not detailed HTTP info)	✅ (Full request info including IP, status)
Useful for audits	✅ Security & compliance audits	✅ Usage and access pattern analysis
Useful for security	✅ Tracks user actions, permission changes	✅ Detects public or suspicious access
Data format	JSON events	Plain text logs

### Summary:

- Use **CloudTrail** to know **who did what** to your S3 resources at the API level.
- Use **Server Access Logs** to know **how the bucket is being accessed** at the HTTP request level (including anonymous/public requests).

Together, they provide a **complete picture** of S3 usage, security, and access for **auditing, troubleshooting, and monitoring**.

### ◆ 10. What is the use of S3 Access Logs and how do you set it up?

- Logs details of **who accessed what, when, and how** ✓
- Helps in **security audits, billing analysis, and performance troubleshooting** ✓
- Set it up by enabling **server access logging** and specifying a target bucket ✓
- Ensure proper **permissions on the target bucket** ✓
- Be aware of potential **logging latency** (logs may take hours to deliver) ✓
- Consider **log file prefix** for better organization ✓
- Plan for **log analysis tools** like Athena or Amazon OpenSearch ✓

**Which tool provides a history of API calls made to your S3 bucket?**

- A. AWS CloudTrail
- B. CloudWatch
- C. S3 Lifecycle Rules
- D. IAM Policy Simulator

---

**What needs to be enabled in S3 to track all access requests to a bucket?**

- A. S3 Object Lock
- B. Server Access Logging
- C. Lambda Trigger
- D. Static Website Hosting

 **Answer: B. Server Access Logging**

---

---