



1 Introduction

- 1 CloudTrail data events provide detailed logs of all actions performed on objects within your S3 buckets.
- 2 This includes actions like GetObject (downloading), PutObject (uploading), DeleteObject, and more.
- 3 This granularity allows you to see exactly who accessed which objects, when, and from where.

2 S3 Server Access Logging VS CloudTrail data events

1 Server Access Logging

- 1 Primary Focus
 - 1 Provides a summary-level log of requests made to your S3 buckets
 - 1 Requester
 - 2 Request time
 - 3 Request action
 - 4 Response status
 - 6 Error codes
 - 2 Which includes information about
 - 3 Example Log Entry for PutObject (Creating a New Object): 79a5d7c4c5d64ad20a0b20dfd3f53d57 3a9e2342bafdad28 [19/Jun/2024:12:00:00 +0000] 192.0.2.0 arn:aws:iam::123456789012:user/ExampleUser EXAMPLE REST.PUT.OBJECT example-bucket/new-object.txt "PUT /example-bucket/new-object.txt HTTP/1.1" 200 - 1024 - 3a9e2342bafdad28 - S3Console -
- 2 Log Format Plain text
- 3 Configuration Configured at the bucket level, specify target bucket for logs
- 4 Performance Impact Minimal, but high-traffic buckets can generate significant log data
- 5 Use Cases Auditing access requests, debugging issues, analyzing traffic patterns

2 CloudTrail data events

- 1 Primary Focus
 - 1 Detailed logging of API activities for compliance, governance, and operational auditing
 - 2 Which includes information about Detailed API calls including object-level operations like GetObject, PutObject, DeleteObject
 - 3 AWS CloudTrail Data Events Log Example for PutObject Operation
- 2 Log Format JSON
- 3 Configuration Configured through CloudTrail, enable logging for specific S3 buckets and API events
- 4 Performance Impact Higher due to detailed logging, can generate substantial log data and incur more costs
- 5 Use Cases Security monitoring, compliance auditing, detailed tracking of API activities

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EXAMPLEPRINCIPALID",
    "arn": "arn:aws:iam::123456789012:user/ExampleUser",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLEACCESSKEY",
    "userName": "ExampleUser"
  },
  "eventTime": "2024-06-19T12:00:00Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-sdk-go/1.34.14 (go1.14; linux; amd64)",
  "requestParameters": {
    "bucketName": "example-bucket",
    "key": "new-object.txt"
  },
  "responseElements": {
    "x-amz-request-id": "EXAMPLEREQUESTID",
    "x-amz-id-2": "EXAMPLEID2"
  },
  "additionalEventData": {
    "bytesTransferredIn": 1024
  },
  "requestID": "EXAMPLEREQUESTID",
  "eventID": "EXAMPLEEVENTID",
  "readOnly": false,
  "resources": [
    {
      "type": "AWS::S3::Object",
      "ARN": "arn:aws:s3:::example-bucket/new-object.txt"
    }
  ],
  "eventType": "AwsApiCall",
  "readOnly": false,
  "recipientAccountId": "123456789012"
}
```