

During an audit, you need to prove who accessed sensitive payroll PDFs stored in S3. Which CloudTrail feature should you enable?

## **Answer:**

To track **who accessed which objects in S3**, I would enable **S3 data events** in CloudTrail:

- 1. Go to CloudTrail → Trails
- 2. Choose or create a trail
- 3. Under "Data Events", choose S3
- 4. Specify:
  - Specific S3 buckets (like the sensitive one)
  - o Or all buckets (not recommended due to cost)

## This will log:

- GetObject, PutObject, DeleteObject calls
- Who accessed the object, and when

During an audit, you need to prove who accessed sensitive payroll PDFs stored in S3. Which CloudTrail feature should you enable?

- A. S3 Management Events in CloudTrail
- B. S3 Access Logs
- C. S3 Data Events in CloudTrail
- D. CloudWatch Metrics

Correct Answer: C. S3 Data Events in CloudTrail

**Explanation:** Data events capture object-level operations (GetObject, PutObject, DeleteObject) in S3, which is required for auditing sensitive files.

## Which of the following statements is TRUE about S3 Data Events in CloudTrail?

- A. They are enabled by default for all S3 buckets.
- B. They capture bucket-level activities such as CreateBucket and DeleteBucket.
- C. They capture object-level activities such as GetObject and PutObject.
- D. They cannot be filtered to specific buckets.

Correct Answer: C. They capture object-level activities such as GetObject and PutObject.

## **Explanation:**

Data events are not enabled by default (must be turned on).

- Management events capture bucket-level operations, not data events.
- You can filter Data Events to specific buckets (to control costs).