A user accidentally deleted an S3 bucket. How will you find out who did it and when?

I'd use **CloudTrail logs** to investigate:

1. Go to the **CloudTrail console**
2. Use the **Event history** search
3. Filter by:
    - **Event name**: DeleteBucket
    - **Resource type**: AWS::S3::Bucket
    - Specify the **time window** when the deletion likely happened

The event log will show:

- **Who** performed the action (user or role)
- **When** it happened (timestamp)
- **Source IP**, region, and user agent (e.g., AWS CLI)

Example:
I once used this to trace accidental deletion of a test bucket during cleanup by a developer who had wildcard permissions on S3. We later added resource-level conditions to prevent it.
Follow up: what action will you take ? 1. Version S3, recover 2. If not, then version, backup 3. Check if that guy really need delete permission, remove permission, give only min IAM permission.

A user reports that an S3 bucket has been accidentally deleted. Which AWS service will help you identify *who deleted the bucket and when*?
A. AWS Config
B. AWS CloudTrail
C. S3 Server Access Logs
D. AWS Trusted Advisor

Answer: ✅ B. AWS CloudTrail

After confirming a developer accidentally deleted a non-critical test bucket, what is the **best corrective action** to prevent similar incidents in the future?

A. Enable S3 versioning for the bucket
B. Revoke s3:DeleteBucket from IAM policies and enforce least privilege
C. Use S3 server access logs for all buckets
D. Enable AWS Trusted Advisor for bucket monitoring

Answer: ✅ B. Revoke s3:DeleteBucket and enforce least privilege

---