# AWS CloudTrail S3 Bucket Deletion Investigation

This document walks through an incident investigation conducted via Kibana (ELK) using CloudTrail logs ingested from AWS.

---

## 🎯 Objective

Investigate unauthorized or unusual S3 bucket deletion using CloudTrail logs parsed via Filebeat into Kibana.

---

## 🏁 Initial Setup

- CloudTrail logs were delivered to S3
- Filebeat forwarded logs into Elasticsearch (via `filebeat-aws` module)
- Kibana used to search within `filebeat-*` index

---

## 🪝 KQL Query for Investigation

event.dataset: aws.cloudtrail and event.provider: "s3.amazonaws.com" and aws.cloudtrail.request_parameters: *appbackupfilesbuk* and event.action : *

---

## 🕵️ Findings Summary

- **Action:** `DeleteBucket`

- **Bucket Name:** `appbackupfilesbuk`
- **Time of Deletion:** `2025-01-30T10:20:19Z`
- **User Involved:** `HelpdeskAdmin`
- **Source IP:** `36.255.87.7`
- **Region:** `ap-south-1`
- **Tool Used:** `aws-cli` on Windows 10

---

## 📊 Log Summary Extract (Simplified)

```
{
  "event.action": "DeleteBucket",
  "user.name": "HelpdeskAdmin",
  "source.ip": "36.255.87.7",
  "event.outcome": "success",
  "aws.cloudtrail.read_only": false,
  "aws.cloudtrail.request_parameters.bucketName": "appbackupfilesbuk"
}
```

---

## 📌 Why Bucket Name Matters

`appbackupfilesbuk` was identified in the CloudTrail logs as the target of the `DeleteBucket` API call. Investigating this bucket confirms whether sensitive data or backups were removed maliciously or unintentionally.

---

## 📥 Artifact

CloudTrail Log Location:

https://aws-cloudtrail-logs-010928207857-58476b9d.s3.ap-south-1.amazonaws.com/AWSLogs/010928207857/CloudTrail/ap-south-1/2025/01/30/010928207857_CloudTrail_ap-south-1_20250130T1025Z_vSPPLosclyebdNwq.json.gz

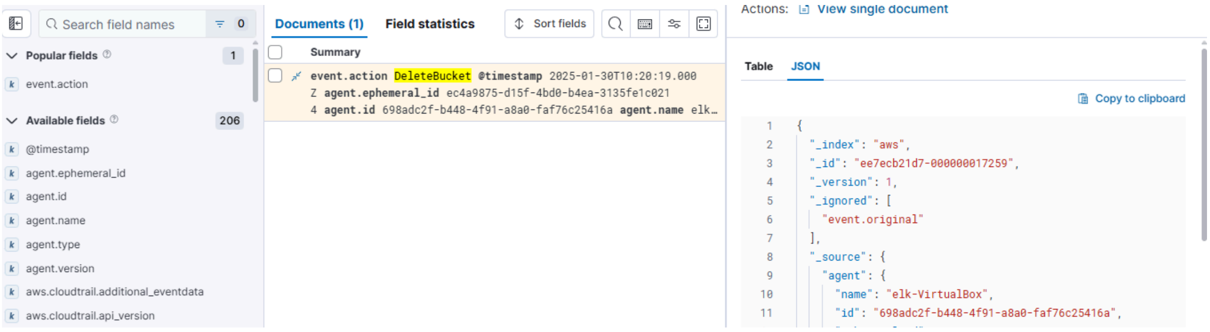
---

# ✅ Conclusion

The IAM user `HelpdeskAdmin` deleted the S3 bucket `appbackupfilesbuk` from a suspicious external IP using AWS CLI. This activity is suspicious and should be flagged for further review and potential IAM role review.

---

[PICS:]



Summary

```
event.action DeleteBucket @timestamp 2025-01-30T10:20:19.000
Z agent.ephemeral_id ec4a9875-d15f-4bd0-b4ea-3135fe1c021
4 agent.id 698adc2f-b448-4f91-a8a0-faf76c25416a agent.name elk…
```

```json
{
  "_index": "aws",
  "_id": "ee7ecb21d7-000000017259",
  "_version": 1,
  "_ignored": [
    "event.original"
  ],
  "_source": {
    "agent": {
      "name": "elk-VirtualBox",
      "id": "698adc2f-b448-4f91-a8a0-faf76c25416a",
```