AWS CloudTrail + S3 + SQS + Filebeat Setup for Centralized Logging

This guide walks through the step-by-step process to set up centralized AWS CloudTrail logging using S3, SQS, and Filebeat to forward logs to ELK (Kibana).

📌 Objective

Enable AWS CloudTrail logs to be delivered via S3 → SQS → Filebeat → Elasticsearch (Kibana) for monitoring and investigation.

🧰 Pre-Requisites

- AWS Account access with IAM privileges
- Ubuntu EC2 instance (for Filebeat)
- ELK stack (running locally or in cloud)

🔧 Step-by-Step Configuration

Step 1: Create an S3 Bucket

- Go to **S3** → **Create bucket**
- Bucket name: `aws-cloudtrail-logs-YOUR_ACCOUNT_ID-uniqueid`
- Region: `ap-south-1`
- Enable **versioning** (recommended)
- Permissions: block all public access ✅

Step 2: Create a CloudTrail Trail

- Go to **CloudTrail** → **Trails** → **Create trail**
- Trail name: `OrgTrail` or `DexterTrail`
- Enable for all regions ✅
- Destination S3 bucket: Select the bucket created above
- Log file validation: Enabled
- Enable CloudWatch logs (optional)

Step 3: Create an SQS Queue

- Go to **SQS** → **Create queue**
- Type: Standard
- Name: `cloudtrail-sqs-queue`

Step 3.1: Add Permissions to SQS

- Attach a policy to allow S3 to send messages:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"Service": "s3.amazonaws.com"},
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:ap-south-1:ACCOUNT_ID:cloudtrail-sqs-queue",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::aws-cloudtrail-logs-ACCOUNT_ID-*"
        }
      }
    }
  ]
}
```

📄 Step 4: Configure Filebeat on EC2

Step 4.1: Install Filebeat

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.17.0-amd64.deb
sudo dpkg -i filebeat-8.17.0-amd64.deb
```

Step 4.2: Update Filebeat Configuration

Path: `/etc/filebeat/filebeat.yml`

Update the following section:

```
filebeat.inputs:
- type: aws-s3
  queue_url: https://sqs.ap-south-1.amazonaws.com/ACCOUNT_ID/cloudtrail-sqs-queue
  access_key_id: YOUR_ACCESS_KEY
  secret_access_key: YOUR_SECRET_KEY
  bucket_arn: arn:aws:s3:::aws-cloudtrail-logs-ACCOUNT_ID-uniqueid
  file_selectors:
```

```
  - regex: ".*CloudTrail.*\.json\.gz"
```

Add Elasticsearch output:

```
output.elasticsearch:
  hosts: ["http://localhost:9200"]
```

Step 4.3: Start Filebeat

```
sudo systemctl enable filebeat
sudo systemctl start filebeat
```

✅ Step 5: Verify in Kibana

- Go to Kibana → Discover
- Index pattern: `filebeat-*`
- Use query:

```
event.module : "aws" and event.dataset : "aws.cloudtrail"
```

- You should see CloudTrail logs being ingested

📦 Output Example (Log snippet)

```
{
  "event.action": "DeleteBucket",
  "user.name": "HelpdeskAdmin",
  "source.ip": "36.255.87.7",
  "cloud.region": "ap-south-1",
  "event.outcome": "success"
}
```
