
Log Search Example: Grouping and Sorting Events

☑ **Step 1: Run the Query**

```
_sourceCategory=labs/aws/cloudtrail
| json field=_raw "eventName"
| count by eventName
| sort by _count desc
```

🔑 **Query Breakdown**

1. **_sourceCategory=labs/aws/cloudtrail**
    - Filters logs to only show data from the labs/aws/cloudtrail source category.
2. **json field=_raw "eventName"**
    - Extracts the field **eventName** (e.g., ConsoleLogin, CreateBucket, RunInstances).
3. **count by eventName**
    - Groups logs by **unique event names**.
    - Counts the number of occurrences for each event.
    - Produces a summary table instead of raw log lines.
4. **sort by _count desc**
    - Sorts the summary table in **descending order** by _count.
    - This means the **most frequent events appear at the top** of the results.
    - Helps prioritize analysis by showing high-volume activities first.

📌 **Importance of count by + sort by**

- **count by** → Aggregates raw logs into meaningful summaries.
- **sort by _count desc** → Organizes the results so analysts see the **most common events immediately**.
- Together, they provide **both insight and prioritization**.

📖 **Summary:**
The combination of **count by** and **sort by _count desc** is a best practice for log analysis. It not only summarizes repetitive events but also orders them by frequency, allowing SOC analysts to quickly detect common patterns and spot anomalies.
