
Log Search Example: Identify Most Active Users

✅ **Step 2: Run the Query**

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

🔎 **Query Breakdown**

1. **_sourceCategory=labs/aws/cloudtrail**
    - Filters logs to only include data from AWS CloudTrail events in the labs/aws/cloudtrail category.
2. **json field=_raw "userIdentity.userName"**
    - Extracts the userName field from the userIdentity object inside the raw log.
    - This value represents the AWS **user account** that performed the action (e.g., AdminUser, EC2ServiceRole, Alice).
3. **count by userIdentity.userName**
    - Groups all logs by the extracted userName.
    - Counts the number of actions/events each user generated.
    - Summarizes activity per user instead of showing raw logs.
4. **sort by _count desc**
    - Sorts the results by frequency in descending order.
    - Users with the **most activity appear at the top** of the results.
    - Helps identify the **most active or potentially suspicious accounts**.

📌 **Importance of This Query**

- **Detect Usage Patterns:** Quickly see which AWS users are generating the most events.
- **Spot Anomalies:** If a service account or low-privileged user suddenly has unusually high activity, it might indicate compromise.

- **Prioritize Investigations:** High-frequency users can be reviewed first to ensure activity is legitimate.

📖 **Summary:**
This query helps analysts **profile user activity** by counting how many CloudTrail events each AWS user generated. The **count by** operator groups data per user, while **sort by _count desc** highlights the **most active accounts immediately**.