

Metadata Tag: `_sourceCategory`

- `_sourceCategory` is a **metadata tag** in Sumo Logic that helps organize and filter logs.
- Think of it as a **label** that tells you *where the log came from* (e.g., `labs/aws/cloudtrail`, `prod/web/app`, `dev/db/mysql`).
- **Importance:**
 - Makes it easy to narrow searches to only the logs you care about.
 - Helps build **dashboards and alerts** based on specific environments or applications.
 - Provides **structure** in large environments where logs come from many different systems.
-  Example:
- `_sourceCategory=prod/web/app`

→ This limits results to logs from the production web application.

Search Operators in Sumo Logic

1. **AND**

- Returns results that contain **all specified terms**.
- Example:
- `error AND timeout`

→ Finds logs that contain both *error* and *timeout*.

2. **OR**

- Returns results that contain **either one term or the other**.
- Example:
- `error OR warning`

→ Finds logs that contain either *error* or *warning*.

3. **Wildcard (*)**

- Matches **any string of characters**.
- Useful when you don't know the exact value.


- Example:
- user=*


→ Matches logs with any user value (e.g., user=Admin, user=Alice).

- Example with prefix:
- _sourceCategory=prod/web/*

→ Includes all logs from categories starting with prod/web/.

LiveTail in Sumo Logic

- **LiveTail** lets you **stream logs in real-time** as they arrive in Sumo Logic.
 - Similar to running tail -f on a Linux log file, but across all ingested data sources.
 - **Why it's useful:**
 - Instant visibility into what's happening right now.
 - Great for troubleshooting incidents or debugging deployments.
 - Lets teams watch logs **together in real-time** during an investigation.
 -  Example Use Case:
 - You deploy a new web service → open LiveTail on its _sourceCategory → instantly see errors, warnings, or successful API calls as they happen.
-

 These three concepts (_sourceCategory, operators, LiveTail) are **fundamentals for SOC analysts and engineers**, because they let you:

- **Filter** logs effectively,
 - **Build precise queries**,
 - **Respond in real-time** when incidents occur.
-