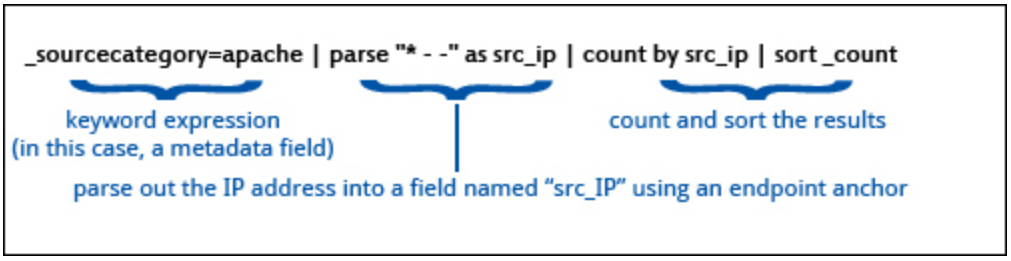
# 1.1.2 Built-in Metadata.md

github.com/aniket0609/Sumo_Logic_basic/blob/main/1.1.2 Built-in Metadata.md




## Built-in Metadata

Sumo Logic has several metadata fields that are automatically tagged to ingested data. These metadata fields are referenced by the service in many ways, such as the user interface when managing Collection, and can be referenced in search queries.

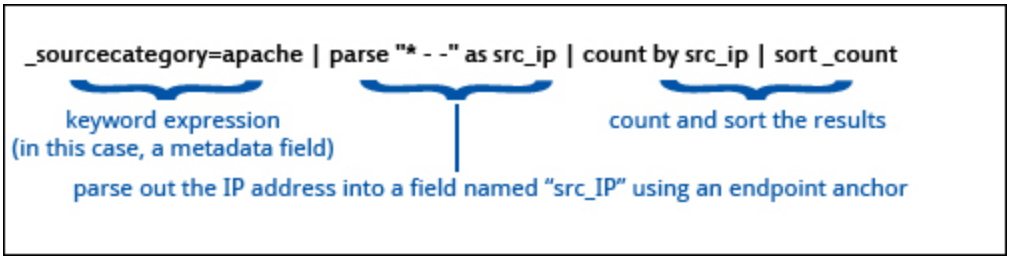
Built-in metadata fields You can run queries using any of the following built-in metadata fields:

| Name | Description |
|---|---|
| `_collector` | The name of the Collector (set when the Collector was installed) that received the log message. |
| `_messageCount` | A sequence number (per Source) added by the Collector when the message was received. |
| `_messageTime` | The parsed timestamp by the Collector from the log message in milliseconds. If the message does not have a timestamp, messageTime uses the receiptTime. |
| `_raw` | The raw log message. |
| `_receiptTime` | The time the Collector received the message in milliseconds. |
| `_size` | The size of the log message in bytes. |
| `_source` | The name of the Source, determined by the name you entered when you configured the Source. |
| `_sourceCategory` | The category of the Source that collected the log message. This can be a maximum of 1,024 characters. |
| `_sourceHost` | The host name of the Source. For local Sources the name of the Source is set when you configure the Source. For remote Collectors, this field uses the remote host's name.The `_sourceHost` metadata field is populated using a reverse DNS lookup. If the name cannot be resolved, `_sourceHost` is displayed as localhost. This can be a maximum of 128 characters. |

| Name | Description |
|---|---|
| `_sourceName` | The name of the log file, determined by the path you entered when you configured the Source. |
| `_format` | The pattern used for parsing the timestamp. |
| `_view` | The name of the index, view, or partition. |

Searching metadata

To run a search using metadata fields:




1.As part of the keyword expression before the first pipe, enter the metadata field name.

2.Add an equals sign (=).

3.Add the metadata value you want to search against. A few tips:

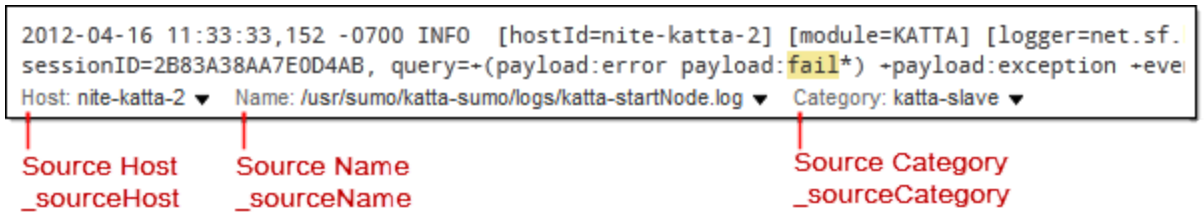
- Add wildcards at the front and back of any partial term or string to capture the most results.
- If your metadata value contains spaces wrap it in quotes `" "`.
- Quotes and wildcards cannot be used together.
- Metadata tags `E.g._sourceHost` are case-insensitive when searching.

This table shows some examples and a description of each metadata type.

| Example | Description |
|---|---|
| `_collector=Mac_server`<br>`_collector=AWS_1*` | Returns results from the named Collector only. Entered when a Collector is installed and activated. |
| `_source=main_web_app`<br>`_source=*syslog*` | Returns results from the named Source only. Entered when a Source is configured. |
| `_sourceCategory=*apache*`<br>`_sourceCategory="Security Logs"` | Returns results from one or more Sources depending on whether the tag was applied to a single Source or a series of Sources. Entered when a Source is configured. |

| Example | Description |
| --- | --- |
| `_sourceHost=hostname`<br>`_sourceHost=*RAS*` | Usually returns results from one Source, unless a value is entered at the Collector level for a Collector with more than one Source.If the field is left blank when a Source is configured, the value for Source Host is taken from the host system value. A custom value can be entered at the Source or Collector configuration. Metadata values entered at Source level override Collector values. |
| `_sourceName=path/to/file/`<br>`_sourceName=*path*` | Returns results from one or more Source paths. Entered when a Source is configured. Note that the metadata field _sourceName is not the name of the Source, but the file path. |
| `_view=sumologic_default` | Returns results more quickly and efficiently because the search runs against a smaller data set. This is a separate subsets of data in your account where you put your special kind data. |

In the Messages tab, each message displays its metadata tags:




msg-with-metadata Search different values of a metadata field in the same query To search more than one value of the same metadata field, you can use the conditional operator OR. Metadata fields follow the same rules as Keyword Search Expressions.

For example:

```
(_sourceCategory=*apache* or _sourceCategory="Security Logs")
```