About Search Basics

Our Search Syntax is based on a funnel or "pipeline" concept. The wide mouth of the funnel begins with all your current Sumo Logic data, and you narrow the funnel by entering keywords and operators separated by pipes ("|"). Each operator acts on the results from the previous operator so that you can progressively filter and pinpoint your search until you find exactly what you're looking for.

In the Search tab, a search query is typically formatted something like this:

```
keyword search | parse | where | group-by | sort | limit
```

Let's start with a basic search:

1. Click the + New button in the tab bar and select Log Search.

![Image of the Log Search button](image)

2. Enter a simple key term like "error" in the search field, or type an asterisk wildcard (*) to find all messages.

3. Hit Enter or click Start.

4. Sumo Logic returns all the log entries containing the search term in the Messages tab below the histogram.

Now let's take a look at a slightly more complex search query to see how queries are formed.

All queries begin with a keyword or string search. Wildcards are allowed including an asterisk (*) for zero or more characters and a question mark (?) for a single character. Strings can be parsed based on start and stop anchor points in messages, and then aliased as user-created fields. All operators are separated by the pipe symbol (|).

Here's an example:

```
_sourcecategory=apache | parse "* --" as src_ip | count by src_ip | sort _count
```

Broken up, this means:

```
_sourcecategory=apache | parse "* --" as src_ip | count by src_ip | sort _count
```

Copyright 2022 Sumo Logic, Inc. All rights reserved.
As queries get longer and more complex, it is a best practice to format your queries by using a soft return before the pipes, such as:

\[ \_sourcecategory=apache \]
\[ \_parse "\* --" as src\_ip \]
\[ \_count by src\_ip \]
\[ \_sort \_count \]

This method lines up the pipes and makes your query much easier to read.
Searches can be long and complex, but they are limited to a maximum of 15,000 characters.

---

See also

- Learn more about [How to Build a Search](#).
- Expand the complexity of your search queries with Sumo Logic [search operators](#).
- [Save a search](#) to re-use later or to run as regularly [scheduled searches](#) that can be delivered to your email address.
- [Share a link](#) to the results of a search query, depending on each user's permissions. To share a link to a search, after your query has run, click **Share** beneath the search query box. This link will be available for three years after it is created.
- See [Best Practices: Search Rules to Live By](#) for types on writing efficient searches.