Lab 1 - Search Basics: Metadata and Keywords

This lab teaches you how to start with the first line of query by using metadata and keywords.

In this lab, you will learn the use of metadata and keywords to narrow your search scope and improve performance.

1. Search for all messages with _sourceCategory=Labs/Apache/Access for the last 15 minutes.

   _sourceCategory=Labs/Apache/Access

2. To identify client errors, narrow your search for only those with "404".

   _sourceCategory=Labs/Apache/Access AND 404

3. Use Boolean logic to search for log lines matching "Error" or "check" or "checkout".

   _sourceCategory=Labs/Apache/Access AND (Error OR check*)

4. In a new tab, search for messages with _sourceCategory=Labs/Apache/Error for the last 45 minutes (-45m).

   _sourceCategory=Labs/Apache/Error

5. Search across both Labs/Apache/Access and Labs/Apache/Error Source Categories:

   _sourceCategory=Labs/Apache/Error OR _sourceCategory=Labs/Apache/Access

6. Search across both Labs/Apache/Access and Labs/Apache/Error Source Categories using wildcards:

   _sourceCategory=Labs/Apache/*

7. Run a Live Tail search for Labs/Apache/Access for messages containing 404s. Notice Live Tail sessions do support wildcards searches.

   _sourceCategory=Labs/Apache/Access 404
QUIZ: True or False

1. Keywords are case-sensitive

2. AND is implicit and OR is explicit

3. Keywords and metadata can use wildcards for Live tail