multisearch

Description

The multisearch command is a generating command that runs multiple streaming searches at the same time. This command requires at least two subsearches and allows only streaming operations in each subsearch. Examples of streaming searches include searches with the following commands: search, eval, where, fields, and rex. For more information, see Types of commands in the Search Manual.

Syntax

| multisearch <subsearch1> <subsearch2> <subsearch3> ...

Required arguments

<subsearch>

Syntax: "["search <logical-expression>"]"
Description: At least two streaming searches must be specified. See the search command for detailed information about the valid arguments for <logical-expression>.

To learn more, see About subsearches in the Search Manual.

Usage

The multisearch command is an event-generating command. See Command types.

Generating commands use a leading pipe character and should be the first command in a search.

Subsearch processing and limitations

With the multisearch command, the events from each subsearch are interleaved. Therefore the multisearch command is not restricted by the subsearch limitations.

Unlike the append command, the multisearch command does not run the subsearch to completion first. The following subsearch example with the append command is not the same as using the multisearch command.
Examples

**Example 1:**

Search for events from both index a and b. Use the `eval` command to add different fields to each set of results.

```
index=a | eval type = "foo" | append [search index=b | eval mytype = "bar"]
```

See also

append, join

Answers

Have questions? Visit Splunk Answers and see what questions and answers the Splunk community has using the `multisearch` command.