



findkeywords

⚠CAUTION: The `findkeywords` command is an internal, unsupported, experimental command. See [About internal commands](#).

Description

Given some integer labeling of events into groups, finds searches to generate these groups.

Syntax

`findkeywords labelfield=<field>`

Required arguments

labelfield

Syntax: `labelfield=<field>`

Description: A field name.

Usage

Use the `findkeywords` command after the `cluster` command, or a similar command that groups events. The `findkeywords` command takes a set of results with a field (labelfield) that supplies a partition of the results into a set of groups. The command derives a search to generate each of these groups. This search can be saved as an [event type](#).

Examples

Return logs for specific log_level values and group the results

Return all logs where the log_level is DEBUG, WARN, ERROR, FATAL and group the results by cluster count.

```
index=_internal source=*splunkd.log* log_level!=info | cluster  
showcount=t | findkeywords labelfield=cluster_count
```

The screenshot shows a Splunk search interface with the following search bar content:

```
index=_internal source=*splunkd.log* log_level!=info | cluster showcount=t | findkeywords labelfield=cluster_count
```

Below the search bar, it says "15 events (before 8/19/14 7:32:08.000 PM)". The search results are displayed in a table with the following data:

confidence	eventTypeable	excludeKeywords	groupID	includeKeywords	numInInputGroup	numMatched	percentInInputGroup	percentMatched	sampleEvent
0.690309	1		1		12	15	0.800000	1.000000	08-19-2014 14:22:23.512 +0200 WARN Ir /splunkbeta/etc/system/default/searchb parse into key-value pair, if applicable.
0.000000	1		10		1	0	0.066667	0.000000	08-19-2014 14:21:28.096 +0200 WARN C time found in the next 1051200 minutes
0.000000	1		3		1	0	0.066667	0.000000	08-19-2014 18:25:53.478 +0200 ERROR I get info for non-existent user=""
0.000000	1		2		1	0	0.066667	0.000000	08-19-2014 14:20:55.947 +0200 WARN D parse timestamp. Defaulting to timestamp Nov 5 00:00:00 2012. Context: source://etc/apps/splunk_5.2_overview /data/violations_plus.csv:host::splunk_oi

The values of `groupID` are the values of `cluster_count` returned from the `cluster` command.

See also

[cluster](#) , [findtypes](#)