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

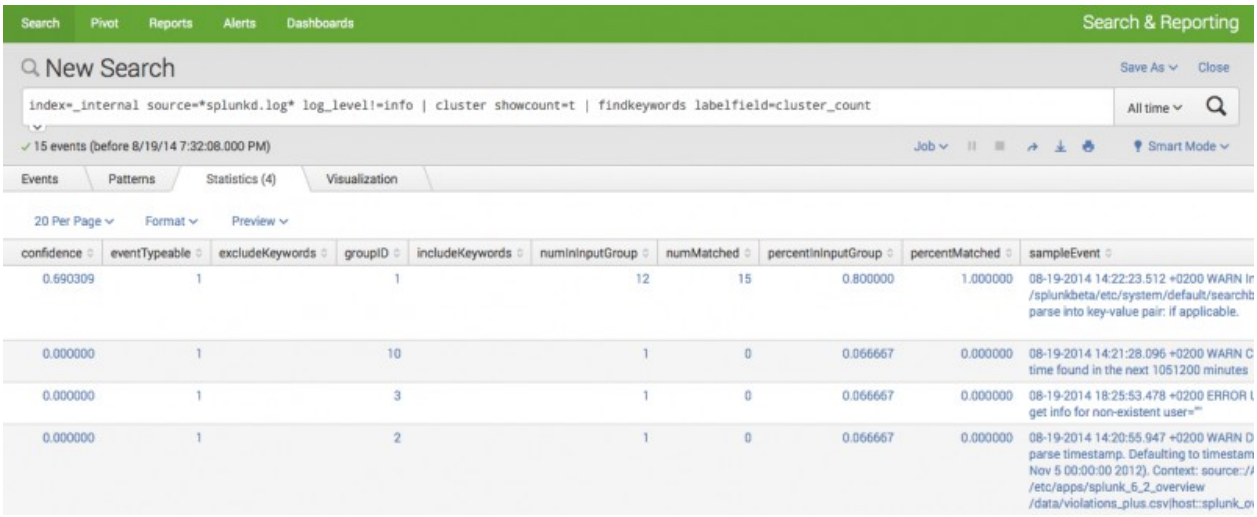
Use the `findkeywords` command after the `cluster` command, or a similar command that groups events. The `findkeyword` command takes a set of results with a field (labelfield) that supplies a partition of the results into a set of groups. The command derives a search to generate each of these groups. 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 values of `groupID` are the values of `cluster_count` returned from the `cluster` command.

See also

cluster , findtypes