Splunk® Enterprise Search Reference 9.0.4

Command types

Generated: 2/15/2023 3:18 am

Command types

There are six broad types for all of the search commands: distributable streaming, centralized streaming, transforming, generating, orchestrating and dataset processing. These types are not mutually exclusive. A command might be streaming or transforming, and also generating.

The following tables list the commands that fit into each of these types. For detailed explanations about each of the types, see Types of commands in the *Search Manual*.

Streaming commands

A **streaming command** operates on each event as the event is returned by a search.

- A distributable streaming command runs on the indexer or the search head, depending on where in the search the command is invoked. Distributable streaming commands can be applied to subsets of indexed data in a parallel manner.
- A centralized streaming command applies a transformation to each event returned by a search. Unlike distributable streaming commands, a centralized streaming command only works on the search head.

Command	Notes
addinfo	Distributable streaming
addtotals	Distributable streaming. A transforming command when used to calculate column totals (not row totals).
arules	Some of the work is distributable streaming running on the indexer or the search head. The rest of the work is centralized streaming running on the search head.
autoregress	Centralized streaming.
bin	Streaming if specified with the `span` argument. Otherwise a dataset processing command.
bucketdir	Distributable streaming by default, but centralized streaming if the `local` setting specified for the command in the commands.conf file is set to true.
cluster	Streaming in some modes.
convert	Distributable streaming.
dedup	Streaming by default. Using the `sortby` argument or specifying `keepevents=true` makes the `dedup` command a dataset processing command.
eval	Distributable streaming.
extract	Distributable streaming.
fieldformat	Distributable streaming.
fields	Distributable streaming.
fillnull	Distributable streaming when a `field-list` is specified. A dataset processing command when no `field-list` is specified.
head	Centralized streaming.
highlight	Distributable streaming.
iconify	Distributable streaming.
iplocation	Distributable streaming.

Command	Notes
join	Centralized streaming, if there is a defined set of fields to join to. A dataset processing command when no `field-list` is specified.
lookup	Distributable streaming when specified with `local=false`, which is the default. An orchestrating command when `local=true`.
makemv	Distributable streaming.
multikv	Distributable streaming.
mvexpand	Distributable streaming.
nomv	Distributable streaming.
rangemap	Distributable streaming.
regex	Distributable streaming.
reltime	Distributable streaming.
rename	Distributable streaming.
replace	Distributable streaming.
rex	Distributable streaming.
search	Distributable streaming if used further down the search pipeline. A generating command when it is the first command in the search.
spath	Distributable streaming.
strcat	Distributable streaming.
streamstats	Centralized streaming.
tags	Distributable streaming.
transaction	Centralized streaming.
typer	Distributable streaming.
where	Distributable streaming.
untable	Distributable streaming.
xmlkv	Distributable streaming.
xmlunescape	Distributable streaming by default, but centralized streaming if the `local` setting specified for the command in the commands.conf file is set to true.
xpath	Distributable streaming.
xyseries	Distributable streaming if the argument `grouped=false` is specified, which is the default. Otherwise a transforming command.

Generating commands

A **generating command** generates events or reports from one or more indexes without transforming the events.

Command	Notes
datamodel	Report-generating
dbinspect	Report-generating.
eventcount	Report-generating.

Command	Notes
from	Can be either report-generating or event-generating depending on the search or knowledge object that is referenced by the command.
gentimes	Event-generating.
inputcsv	Event-generating (centralized).
Inputlookup	Event-generating (centralized) when `append=false`, which is the default.
loadjob	Event-generating (centralized).
makeresults	Report-generating.
metadata	Report-generating. Although metadata fetches data from all peers, any command run after it runs only on the search head.
metasearch	Event-generating.
mstats	Report-generating, except when `append=true` is specified.
multisearch	Event-generating.
pivot	Report-generating.
rest	
search	Event-generating (distributable) when the first command in the search, which is the default. A streaming (distributable) command if used later in the search pipeline.
searchtxn	Event-generating.
set	Event-generating.
tstats	Report-generating (distributable) when `prestats=true`. When `prestats=false`, `tstats` is event-generating.

Transforming commands

A **transforming command** orders the results into a data table. The command "transforms" the specified cell values for each event into numerical values for statistical purposes.

In earlier versions of Splunk software, transforming commands were called reporting commands.

Command	Notes
addtotals	Transforming when used to calculate column totals (not row totals). A distributable streaming command when used to calculate row totals, which is the default.
anomalydetection	
append	
chart	
cofilter	
contingency	
history	
makecontinuous	
mvcombine	
rare	

Command	Notes
stats	
table	
timechart	
top	
xyseries	Transforming if `grouped=true`. A streaming (distributable) command when `grouped=false`, which is the default setting.

Orchestrating commands

Orchestrating commands control some aspect of how a search is processed. They do not directly affect the final result set of the search. For example, you might apply an orchestrating command to a search to enable or disable a search optimization that helps the overall search complete faster.

Command	Notes
localop	
lookup	Only becomes an orchestrating command when `local=true`. This forces the `lookup` command to run on the search head and not on any remote peers. A streaming (distributable) command when `local=false`, which is the default setting.
noop	
redistribute	
require	

Dataset processing commands

A dataset processing command is a command that requires the entire dataset before the command can run. Some of these commands fit into other command types in specific situations or when specific arguments are used.

Command	Notes
anomalousvalue	Some modes
anomalydetection	Some modes
append	Some modes
bin	Some modes. A streaming command if the `span` argument is specified.
cluster	Some modes
concurrency	
datamodel	
dedup	Using the `sortby` argument or specifying `keepevents=true` makes the `dedup` command a dataset processing command. Otherwise, `dedup` is a streaming command.
eventstats	
fieldsummary	
fillnull	When no `field-list` is specified, a dataset processing command. If a `field-list` is specified `fillnull` is a distributable streaming command.
from	Some modes

Command	Notes
join	Some modes. A centralized streaming command when there is a defined set of fields to join to.
map	
outlier	
reverse	
sort	
tail	
transaction	Some modes
union	Some modes