Commands by category

The following tables list all the search commands, categorized by their usage. Some commands fit into more than one category based on the options that you specify.

Correlation

These commands can be used to build correlation searches.

Command	Description
append	Appends subsearch results to current results.
appendcols	Appends the fields of the subsearch results to current results, first results to first result, second to second, etc.
appendpipe	Appends the result of the subpipeline applied to the current result set to results.
arules	Finds association rules between field values.
associate	Identifies correlations between fields.
contingency, counttable, ctable	Builds a contingency table for two fields.
correlate	Calculates the correlation between different fields.
diff	Returns the difference between two search results.
join	Combines the results from the main results pipeline with the results from a subsearch.
lookup	Explicitly invokes field value lookups.
selfjoin	Joins results with itself.
set	Performs set operations (union, diff, intersect) on subsearches.
stats	Provides statistics, grouped optionally by fields. See Statistical and charting functions.
transaction	Groups search results into transactions.

Data and indexes

These commands can be used to learn more about your data, add and delete data sources, or

View data

These commands return information about the data you have in your indexes. They do not modify your data or indexes in any way.

Command	Description
datamodel	Return information about a data model or data model object.
dbinspect	Returns information about the specified index.
eventcount	Returns the number of events in an index.
metadata	Returns a list of source, sourcetypes, or hosts from a specified index or distributed search peer.
typeahead	Returns typeahead information on a specified prefix.

Manage data

These are some commands you can use to add data sources to or delete specific data from your indexes.

Command	Description
delete	Delete specific events or search results.

Manage summary indexes

These commands are used to create and manage your summary indexes.

Command	Description
collect, stash	Puts search results into a summary index.
overlap	Finds events in a summary index that overlap in time or have missed events.
sichart	Summary indexing version of chart. Computes the necessary information for you to later run a chart search on the summary index.
sirare	Summary indexing version of rare. Computes the necessary information for you to later run a rare search on the summary index.
sistats	Summary indexing version of stats. Computes the necessary information for you to later run a stats search on the summary index.
sitimechart	Summary indexing version of timechart. Computes the necessary information for you to later run a timechart search on the summary index.
sitop	Summary indexing version of top. Computes the necessary information for you to later run a top search on the summary index.

Fields

These are commands you can use to add, extract, and modify fields or field values. The most useful command for manipulating fields is eval and its statistical and charting functions.

Add fields

Use these commands to add new fields.

Command	Description
accum	Keeps a running total of the specified numeric field.
addinfo	Add fields that contain common information about the current search.
addtotals	Computes the sum of all numeric fields for each result.
delta	Computes the difference in field value between nearby results.
eval	Calculates an expression and puts the value into a field. See also, evaluation functions.
iplocation	Adds location information, such as city, country, latitude, longitude, and so on, based on IP addresses.
lookup	For configured lookup tables, explicitly invokes the field value lookup and adds fields from the lookup table to the events.
multikv	Extracts field-values from table-formatted events.
rangemap	Sets RANGE field to the name of the ranges that match.
strcat	Concatenates string values and saves the result to a specified field.

Extract fields

These commands provide different ways to extract new fields from search results.

Command	Description
erex	Allows you to specify example or counter example values to automatically extract fields that have similar values.
extract, kv	Extracts field-value pairs from search results.
kvform	Extracts values from search results, using a form template.
rex	Specify a Perl regular expression named groups to extract fields while you search.
spath	Provides a straightforward means for extracting fields from structured data formats, XML and JSON.
xmlkv	Extracts XML key-value pairs.

Modify fields and field values

Use these commands to modify fields or their values.

Command	Description
convert	Converts field values into numerical values.
filldown	Replaces NULL values with the last non-NULL value.
fillnull	Replaces null values with a specified value.
makemv	Change a specified field into a multivalue field during a search.
nomv	Changes a specified multivalue field into a single-value field at search time.
reltime	Converts the difference between 'now' and '_time' to a human-readable value and adds adds this value to the field, 'reltime', in your search results.
rename	Renames a specified field. Use wildcards to specify multiple fields.
replace	Replaces values of specified fields with a specified new value.

Find anomalies

These commands are used to find anomalies in your data. Either search for uncommon or outlying events and fields or cluster similar events together.

Command	Description
analyzefields, af	Analyze numerical fields for their ability to predict another discrete field.
anomalies	Computes an "unexpectedness" score for an event.
anomalousvalue	Finds and summarizes irregular, or uncommon, search results.
anomalydetection	Identifies anomalous events by computing a probability for each event and then detecting unusually small probabilities.
cluster	Clusters similar events together.
kmeans	Performs k-means clustering on selected fields.
outlier	Removes outlying numerical values.
rare	Displays the least common values of a field.

Geographic and location

These commands add geographical information to your search results.

Command	Description
iplocation	Returns location information, such as city, country, latitude, longitude, and so on, based on IP addresses.
geom	Adds a field, named "geom", to each event. This field contains geographic data structures for polygon geometry in JSON and is used for choropleth map visualization. This command requires an external lookup with `external_type=geo` to be installed.
geomfilter	Accepts two points that specify a bounding box for clipping choropleth maps. Points that fall outside of the bounding box are filtered out.
geostats	Generate statistics which are clustered into geographical bins to be rendered on a world map.

Metrics

These commands work with metrics data.

Command	Description
mcollect	Converts events into metric data points and inserts the data points into a metric index on the search head.
meventcollect	Converts events into metric data points and inserts the data points into a metric index on indexer tier.
mpreview, msearch	Provides samples of the raw metric data points in the metric time series in your metrics indexes. Helps you troubleshoot your metrics data.
mstats	Calculates visualization-ready statistics for the `measurement`, `metric_name`, and `dimension` fields in metric indexes.

Prediction and trending

These commands predict future values and calculate trendlines that can be used to create visualizations.

Command	Description
predict	Enables you to use time series algorithms to predict future values of fields.
trendline	Computes moving averages of fields.
x11	Enables you to determine the trend in your data by removing the seasonal pattern.

Reports

These commands are used to build transforming searches. These commands return statistical data tables that are required for charts and other kinds of data visualizations.

Command	Description
addtotals	Computes the sum of all numeric fields for each result.
autoregress	Prepares your events for calculating the autoregression, or moving average, based on a field that you specify.
bin, discretize	Puts continuous numerical values into discrete sets.
chart	Returns results in a tabular output for charting. See also, Statistical and charting functions.
contingency, counttable, ctable	Builds a contingency table for two fields.
correlate	Calculates the correlation between different fields.
eventcount	Returns the number of events in an index.
eventstats	Adds summary statistics to all search results.
gauge	Transforms results into a format suitable for display by the Gauge chart types.
makecontinuous	Makes a field that is supposed to be the x-axis continuous (invoked by `chart` / `timechart`)
mstats	Calculates statistics for the measurement, metric_name, and dimension fields in metric indexes.
outlier	Removes outlying numerical values.
rare	Displays the least common values of a field.
stats	Provides statistics, grouped optionally by fields. See also, Statistical and charting functions.
streamstats	Adds summary statistics to all search results in a streaming manner.
timechart	Create a time series chart and corresponding table of statistics. See also, Statistical and charting functions.
top	Displays the most common values of a field.
trendline	Computes moving averages of fields.
tstats	Performs statistical queries on indexed fields in `tsidx` files.
untable	Converts results from a tabular format to a format similar to `stats` output. Inverse of `xyseries` and `maketable`.
xyseries	Converts results into a format suitable for graphing.

Results

These commands can be used to manage search results. For example, you can append one set of results with another, filter more events from the results, reformat the results, and so on.

Alerting

Use this command to email the results of a search.

Command	Description
sendemail	Emails search results, either inline or as an attachment, to one or more specified email addresses.

Appending

Use these commands to append one set of results with another set or to itself.

Command	Description
append	Appends subsearch results to current results.
appendcols	Appends the fields of the subsearch results to current results, first results to first result, second to second, and so on.
join	SQL-like joining of results from the main results pipeline with the results from the subpipeline.
selfjoin	Joins results with itself.

Filtering

Use these commands to remove more events or fields from your current results.

Command	Description
dedup	Removes subsequent results that match a specified criteria.
fields	Removes fields from search results.
from	Retrieves data from a dataset, such as a data model dataset, a CSV lookup, a KV Store lookup, a saved search, or a table dataset.
mvcombine	Combines events in search results that have a single differing field value into one result with a multivalue field of the differing field.
regex	Removes results that do not match the specified regular expression.
searchtxn	Finds transaction events within specified search constraints.
table	Creates a table using the specified fields.
uniq	Removes any search that is an exact duplicate with a previous result.
where	Performs arbitrary filtering on your data. See also, Evaluation functions.

Formatting

Use these commands to reformat your current results.

Command	Description
fieldformat	Uses `eval` expressions to change the format of field values when they are rendered without changing their underlying values. Does not apply to exported data.
transpose	Reformats rows of search results as columns. Useful for fixing X- and Y-axis display issues with charts, or for turning sets of data into a series to produce a chart.
untable	Converts results from a tabular format to a format similar to `stats` output. Inverse of `xyseries` and `maketable`.
xyseries	Converts results into a format suitable for graphing.

Generating

Use these commands to generate or return events.

Command	Description
gentimes	Returns results that match a time-range.
loadjob	Loads events or results of a previously completed search job.
makeresults	Creates a specified number of empty search results.
mvexpand	Expands the values of a multivalue field into separate events for each value of the multivalue field.
savedsearch	Returns the search results of a saved search.
search	Searches indexes for matching events. This command is implicit at the start of every search pipeline that does not begin with another generating command.

Grouping

Use these commands to group or classify the current results.

Command	Description
cluster	Clusters similar events together.
kmeans	Performs k-means clustering on selected fields.
mvexpand	Expands the values of a multivalue field into separate events for each value of the multivalue field.
transaction	Groups search results into transactions.
typelearner	Generates suggested eventtypes.
typer	Calculates the eventtypes for the search results.

Reordering

Use these commands to change the order of the current search results.

Command	Description
head	Returns the first number n of specified results.
reverse	Reverses the order of the results.
sort	Sorts search results by the specified fields.
tail	Returns the last number N of specified results

Reading

Use these commands to read in results from external files or previous searches.

Command	Description
inputcsv	Loads search results from the specified CSV file.
inputlookup	Loads search results from a specified static lookup table.
loadjob	Loads events or results of a previously completed search job.

Writing

Use these commands to define how to output current search results.

Command	Description
collect, stash	Puts search results into a summary index.
meventcollect	Converts events into metric data points and inserts the data points into a metric index on indexer tier.
mcollect	Converts events into metric data points and inserts the data points into a metric index on the search head.
outputcsv	Outputs search results to a specified CSV file.
outputlookup	Writes search results to the specified static lookup table.
outputtext	Ouputs the raw text field (`_raw`) of results into the `_xml` field.
sendemail	Emails search results, either inline or as an attachment, to one or more specified email addresses.

Search

Command	Description
localop	Run subsequent commands, that is all commands following this, locally and not on a remote peer.
map	A looping operator, performs a search over each search result.
redistribute	Invokes parallel reduce search processing to shorten the search runtime of a set of supported SPL commands.
search	Searches indexes for matching events. This command is implicit at the start of every search pipeline that does not begin with another generating command.
sendalert	invokes a custom alert action.
sendemail	Emails search results, either inline or as an attachment, to one or more specified email addresses.

Subsearch

These are commands that you can use with subsearches.

Command	Description
append	Appends subsearch results to current results.
appendcols	Appends the fields of the subsearch results to current results, first subsearch results to first current results, second to second, and so on.
appendpipe	Appends the result of the subpipeline applied to the current result set to results.
foreach	Runs a templated streaming subsearch for each field in a wildcarded field list.
format	Takes the results of a subsearch and formats them into a single result.
join	Combines the results of a subsearch with the results of a main search.
multisearch	Runs multiple streaming subsearches at the same time.
return	Specifies the values to return from a subsearch.
set	Performs set operations (union, diff, intersect) on subsearches.

Time

Use these commands to search based on time ranges or add time information to your events.

Command	Description
gentimes	Returns results that match a time-range.
localize	Returns a list of the time ranges in which the search results were found.
reltime	Converts the difference between 'now' and '_time' to a human-readable value and adds adds this value to the field, 'reltime', in your search results.