Splunk Search Command Quick Reference

Command	Description	Related commands
`abstract`	Produces a summary of each search result.	`highlight`
`accum`	Keeps a running total of the specified numeric field.	`autoregress, delta, trendline, streamstats`
`addcoltotals`	Computes an event that contains sum of all numeric fields for previous events.	`addtotals, stats`
`addinfo`	Add fields that contain common information about the current search.	`search`
`addtotals`	Computes the sum of all numeric fields for each result.	`addcoltotals`, `stats`
`analyzefields`	Analyze numerical fields for their ability to predict another discrete field.	`anomalousvalue`
`anomalies`	Computes an "unexpectedness" score for an event.	`anomalousvalue`, `cluster`, `kmeans`, `outlier`
`anomalousvalue`	Finds and summarizes irregular, or	`analyzefields`, `anomalies`, `cluster`, `kmeans`, `outlier`

	uncommon, search results.	
anomalydetection	Identifies anomalous events by computing a probability for each event and then detecting unusually small probabilities.	analyzefields, anomalies, anomalousvalue, cluster, kmeans, outlier
append	Appends subsearch results to current results.	appendcols, appendcsv, appendlookup, join, set
appendcols	Appends the fields of the subsearch results to current results, first results to first result, second to second, etc.	append, appendcsv, join, set
appendpipe	Appends the result of the subpipeline applied to the current result set to results.	append, appendcols, join, set
arules	Finds association rules between field values.	associate, correlate
associate	Identifies correlations between fields.	correlate, contingency
audit	Returns audit trail information that is stored in the local audit index.	
autoregress	Sets up data for calculating the moving average.	accum, autoregress, delta, trendline, streamstats

`bin` (bucket)	Puts continuous numerical values into discrete sets.	`chart`, `timechart`
`bucketdir`	Replaces a field value with higher-level grouping, such as replacing filenames with directories.	`cluster`, `dedup`
`chart`	Returns results in a tabular output for charting. See also, Statistical and charting functions.	`bin`, `sichart`, `timechart`
`cluster`	Clusters similar events together.	`anomalies`, `anomalousvalue`, `cluster`, `kmeans`, `outlier`
`cofilter`	Finds how many times field1 and field2 values occurred together.	`associate`, `correlate`
`collect`	Puts search results into a summary index.	`overlap`
`concurrency`	Uses a duration field to find the number of "concurrent" events for each event.	`timechart`
`contingency`	Builds a contingency table for two fields.	`associate`, `correlate`
`convert`	Converts field values into numerical values.	`eval`

`correlate`	Calculates the correlation between different fields.	`associate`, `contingency`
`crawl`	Crawls the filesystem for new sources to index.	`input`
`datamodel`	Examine data model or data model object and search a data model object.	`pivot`
`dbinspect`	Returns information about the specified index.	
`dedup`	Removes subsequent results that match a specified criteria.	`uniq`
`delete`	Delete specific events or search results.	
`delta`	Computes the difference in field value between nearby results.	`accum`, `autoregress`, `trendline`, `streamstats`
`diff`	Returns the difference between two search results.	
`erex`	Allows you to specify example or counter example values to automatically extract fields that have similar values.	`extract`, `kvform`, `multikv`, `regex`, `rex`, `xmlkv`

`eval`	Calculates an expression and puts the value into a field. See also, Evaluation functions.	`where`
`eventcount`	Returns the number of events in an index.	`dbinspect`
`eventstats`	Adds summary statistics to all search results.	`stats`
`extract` (kv)	Extracts field-value pairs from search results.	`kvform`, `multikv`, `xmlkv`, `rex`
`fieldformat`	Expresses how to render a field at output time without changing the underlying value.	`eval`, `where`
`fields`	Removes fields from search results.	
`fieldsummary`	Generates summary information for all or a subset of the fields.	`analyzefields`, `anomalies`, `anomalousvalue`, `stats`
`filldown`	Replaces NULL values with the last non-NULL value.	`fillnull`
`fillnull`	Replaces null values with a specified value.	

findtypes	Generates a list of suggested event types.	typer
folderize	Creates a higher-level grouping, such as replacing filenames with directories.	
foreach	Run a templatized streaming subsearch for each field in a wildcarded field list.	eval
format	Takes the results of a subsearch and formats them into a single result.	
gauge	Transforms results into a format suitable for display by the Gauge chart types.	
gentimes	Generates time-range results.	
geom	Adds a field, named "geom", to each event. This field contains geographic data structures for polygon geometry in JSON and is used for the choropleth map visualization.	geomfilter
geomfilter	Accepts two points that specify a bounding box for clipping a choropleth map. Points that fall outside of the	geom

	bounding box are filtered out.	
`geostats`	Generate statistics which are clustered into geographical bins to be rendered on a world map.	`stats`, `xyseries`
`head`	Returns the first number n of specified results.	`reverse`, `tail`
`highlight`	Highlights the specified terms.	`iconify`
`history`	Returns a history of searches formatted as an events list or as a table.	`search`
`iconify`	Displays a unique icon for each different value in the list of fields that you specify.	`highlight`
`input`	Add or disable sources.	
`inputcsv`	Loads search results from the specified CSV file.	`loadjob`, `outputcsv`
`inputlookup`	Loads search results from a specified static lookup table.	`inputcsv`, `join`, `lookup`, `outputlookup`

`iplocation`	Extracts location information from IP addresses.	
`join`	Combine the results of a subsearch with the results of a main search.	`appendcols, lookup, selfjoin`
`kmeans`	Performs k-means clustering on selected fields.	`anomalies, anomalousvalue, cluster, outlier`
`kvform`	Extracts values from search results, using a form template.	`extract, kvform, multikv, xmlkv, rex`
`loadjob`	Loads events or results of a previously completed search job.	`inputcsv`
`localize`	Returns a list of the time ranges in which the search results were found.	`map, transaction`
`localop`	Run subsequent commands, that is all commands following this, locally and not on remote peers.	
`lookup`	Explicitly invokes field value lookups.	
`makecontinuous`	Makes a field that is supposed to be the x-axis continuous	`chart, timechart`

	(invoked by chart/timechart)	
`makemv`	Change a specified field into a multivalued field during a search.	`mvcombine, mvexpand, nomv`
`makeresults`	Creates a specified number of empty search results.	
`map`	A looping operator, performs a search over each search result.	
`metadata`	Returns a list of source, sourcetypes, or hosts from a specified index or distributed search peer.	`dbinspect`
`metasearch`	Retrieves event metadata from indexes based on terms in the logical expression.	`metadata`, `search`
`multikv`	Extracts field-values from table-formatted events.	
`multisearch`	Run multiple **streaming searches** at the same time.	`append, join`
`mvcombine`	Combines events in search results that have a single differing field value into one result	`mvexpand, makemv, nomv`

	with a multivalue field of the differing field.	
`mvexpand`	Expands the values of a multivalue field into separate events for each value of the multivalue field.	`mvcombine, makemv, nomv`
`nomv`	Changes a specified multivalued field into a single-value field at search time.	`makemv, mvcombine, mvexpand`
`outlier`	Removes outlying numerical values.	`anomalies`, `anomalousvalue`, `cluster`, `kmeans`
`outputcsv`	Outputs search results to a specified CSV file.	`inputcsv`, `outputtext`
`outputlookup`	Writes search results to the specified static lookup table.	`inputlookup`, `lookup`, `outputcsv`, `outputlookup`
`outputtext`	Outputs the raw text field (`_raw`) of results into the `_xml` field.	`outputtext`
`overlap`	Finds events in a summary index that overlap in time or have missed events.	`collect`
`pivot`	Run pivot searches against a particular data model object.	`dbinspect`

`predict`	Enables you to use time series algorithms to predict future values of fields.	`x11`
`rangemap`	Sets RANGE field to the name of the ranges that match.	
`rare`	Displays the least common values of a field.	`sirare, stats, top`
`regex`	Removes results that do not match the specified regular expression.	`rex`, `search`
`relevancy`	Calculates how well the event matches the query.	
`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.	`convert`
`rename`	Renames a specified field; wildcards can be used to specify multiple fields.	
`replace`	Replaces values of specified fields with a specified new value.	

`rest`	Access a REST endpoint and display the returned entities as search results.	
`return`	Specify the values to return from a subsearch.	`format, search`
`reverse`	Reverses the order of the results.	`head, sort, tail`
`rex`	Specify a Perl regular expression named groups to extract fields while you search.	`extract, kvform, multikv, xmlkv, regex`
`rtorder`	Buffers events from real-time search to emit them in ascending time order when possible.	
`savedsearch`	Returns the search results of a saved search.	
`script, run`	Runs an external Perl or Python script as part of your search.	
`scrub`	Anonymizes the search results.	
`search`	Searches indexes for matching events.	

`searchtxn`	Finds transaction events within specified search constraints.	`transaction`
`selfjoin`	Joins results with itself.	`join`
`sendemail`	Emails search results to a specified email address.	
`set`	Performs set operations (union, diff, intersect) on subsearches.	`append, appendcols, join, diff`
`setfields`	Sets the field values for all results to a common value.	`eval`, `fillnull`, `rename`
`sichart`	Summary indexing version of chart.	`chart, sitimechart, timechart`
`sirare`	Summary indexing version of rare.	`rare`
`sistats`	Summary indexing version of stats.	`stats`
`sitimechart`	Summary indexing version of timechart.	`chart, sichart, timechart`
`sitop`	Summary indexing version of top.	`top`

`sort`	Sorts search results by the specified fields.	`reverse`
`spath`	Provides a straightforward means for extracting fields from structured data formats, XML and JSON.	`xpath`
`stats`	Provides statistics, grouped optionally by fields. See also, Statistical and charting functions.	`eventstats, top, rare`
`strcat`	Concatenates string values.	
`streamstats`	Adds summary statistics to all search results in a streaming manner.	`eventstats, stats`
`table`	Creates a table using the specified fields.	`fields`
`tags`	Annotates specified fields in your search results with tags.	`eval`
`tail`	Returns the last number n of specified results.	`head, reverse`
`timechart`	Create a time series chart and corresponding table of statistics. See	`chart, bucket`

	also, Statistical and charting functions.	
top	Displays the most common values of a field.	rare, stats
transaction	Groups search results into transactions.	
transpose	Reformats rows of search results as columns.	
trendline	Computes moving averages of fields.	timechart
tscollect	Writes results into tsidx file(s) for later use bytstats command.	collect, stats, tstats
tstats	Calculates statistics over tsidx files created with the tscollect command.	stats, tscollect
typeahead	Returns typeahead information on a specified prefix.	
typelearner	Generates suggested eventtypes.	typer
typer	Calculates the eventtypes for the search results.	typelearner

`uniq`	Removes any search that is an exact duplicate with a previous result.	`dedup`
`untable`	Converts results from a tabular format to a format similar to `stats` output. Inverse of `xyseries` and `maketable`.	
`where`	Performs arbitrary filtering on your data. See also, Evaluations functions.	`eval`
`x11`	Enables you to determine the trend in your data by removing the seasonal pattern.	`predict`
`xmlkv`	Extracts XML key-value pairs.	`extract, kvform, multikv, rex`
`xmlunescape`	Unescapes XML.	
`xpath`	Redefines the XML path.	
`xyseries`	Converts results into a format suitable for graphing.	