

# Splunk Search Commands

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

<a href="#">anomalydetection</a>	Identifies anomalous events by computing a probability for each event and then detecting unusually small probabilities.	<a href="#">analyzefields</a> , <a href="#">anomalies</a> , <a href="#">anomalousvalue</a> , <a href="#">cluster</a> , <a href="#">kmeans</a> , <a href="#">outlier</a>
<a href="#">append</a>	Appends subsearch results to current results.	<a href="#">appendcols</a> , <a href="#">appendcsv</a> , <a href="#">appendlookup</a> , <a href="#">join</a> , <a href="#">set</a>
<a href="#">appendcols</a>	Appends the fields of the subsearch results to current results, first results to first result, second to second, etc.	<a href="#">append</a> , <a href="#">appendcsv</a> , <a href="#">join</a> , <a href="#">set</a>
<a href="#">appendpipe</a>	Appends the result of the subpipeline applied to the current result set to results.	<a href="#">append</a> , <a href="#">appendcols</a> , <a href="#">join</a> , <a href="#">set</a>
<a href="#">arules</a>	Finds association rules between field values.	<a href="#">associate</a> , <a href="#">correlate</a>
<a href="#">associate</a>	Identifies correlations between fields.	<a href="#">correlate</a> , <a href="#">contingency</a>
<a href="#">audit</a>	Returns audit trail information that is stored in the local audit index.	
<a href="#">autoregress</a>	Sets up data for calculating the moving average.	<a href="#">accum</a> , <a href="#">autoregress</a> , <a href="#">delta</a> , <a href="#">trendline</a> , <a href="#">streamstats</a>
<a href="#">bin</a> (bucket)	Puts continuous numerical values into discrete sets.	<a href="#">chart</a> , <a href="#">timechart</a>

<a href="#">bucketdir</a>	Replaces a field value with higher-level grouping, such as replacing filenames with directories.	<code>cluster</code> , <code>dedup</code>
<a href="#">chart</a>	Returns results in a tabular output for charting. See also, <a href="#">Statistical and charting functions</a> .	<code>bin</code> , <code>sichart</code> , <code>timechart</code>
<a href="#">cluster</a>	Clusters similar events together.	<code>anomalies</code> , <code>anomalousvalue</code> , <code>cluster</code> , <code>kmeans</code> , <code>outlier</code>
<a href="#">cofilter</a>	Finds how many times field1 and field2 values occurred together.	<code>associate</code> , <code>correlate</code>
<a href="#">collect</a>	Puts search results into a summary index.	<code>overlap</code>
<a href="#">concurrency</a>	Uses a duration field to find the number of "concurrent" events for each event.	<code>timechart</code>
<a href="#">contingency</a>	Builds a contingency table for two fields.	<code>associate</code> , <code>correlate</code>
<a href="#">convert</a>	Converts field values into numerical values.	<code>eval</code>
<a href="#">correlate</a>	Calculates the correlation between different fields.	<code>associate</code> , <code>contingency</code>
<a href="#">crawl</a>	Crawls the filesystem for new sources to index.	<code>input</code>

<code>datamodel</code>	Examine data model or data model object and search a data model object.	<code>pivot</code>
<code>dbinspect</code>	Returns information about the specified index.	
<code>dedup</code>	Removes subsequent results that match a specified criteria.	<code>uniq</code>
<code>delete</code>	Delete specific events or search results.	
<code>delta</code>	Computes the difference in field value between nearby results.	<code>accum</code> , <code>autoregress</code> , <code>trendline</code> , <code>streamstats</code>
<code>diff</code>	Returns the difference between two search results.	
<code>erex</code>	Allows you to specify example or counter example values to automatically extract fields that have similar values.	<code>extract</code> , <code>kvform</code> , <code>multikv</code> , <code>regex</code> , <code>rex</code> , <code>xmlkv</code>
<code>eval</code>	Calculates an expression and puts the value into a field. See also, <a href="#">Evaluation functions</a> .	<code>where</code>
<code>eventcount</code>	Returns the number of events in an index.	<code>dbinspect</code>

<code>eventstats</code>	Adds summary statistics to all search results.	<code>stats</code>
<code>extract</code> (kv)	Extracts field-value pairs from search results.	<code>kvform</code> , <code>multikv</code> , <code>xmlkv</code> , <code>rex</code>
<code>fieldformat</code>	Expresses how to render a field at output time without changing the underlying value.	<code>eval</code> , <code>where</code>
<code>fields</code>	Removes fields from search results.	
<code>fieldsummary</code>	Generates summary information for all or a subset of the fields.	<code>analyzefields</code> , <code>anomalies</code> , <code>anomalousvalue</code> , <code>stats</code>
<code>filldown</code>	Replaces NULL values with the last non-NULL value.	<code>fillnull</code>
<code>fillnull</code>	Replaces null values with a specified value.	
<code>findtypes</code>	Generates a list of suggested event types.	<code>typer</code>
<code>folderize</code>	Creates a higher-level grouping, such as replacing filenames with directories.	
<code>foreach</code>	Run a templated streaming subsearch for each field in a wildcarded field list.	<code>eval</code>

<code>format</code>	Takes the results of a subsearch and formats them into a single result.	
<code>gauge</code>	Transforms results into a format suitable for display by the Gauge chart types.	
<code>gentimes</code>	Generates time-range results.	
<code>geom</code>	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.	<code>geomfilter</code>
<code>geomfilter</code>	Accepts two points that specify a bounding box for clipping a choropleth map. Points that fall outside of the bounding box are filtered out.	<code>geom</code>
<code>geostats</code>	Generate statistics which are clustered into geographical bins to be rendered on a world map.	<code>stats</code> , <code>xyseries</code>
<code>head</code>	Returns the first number n of specified results.	<code>reverse</code> , <code>tail</code>
<code>highlight</code>	Highlights the specified terms.	<code>iconify</code>

<code>history</code>	Returns a history of searches formatted as an events list or as a table.	<code>search</code>
<code>iconify</code>	Displays a unique icon for each different value in the list of fields that you specify.	<code>highlight</code>
<code>input</code>	Add or disable sources.	
<code>inputcsv</code>	Loads search results from the specified CSV file.	<code>loadjob</code> , <code>outputcsv</code>
<code>inputlookup</code>	Loads search results from a specified static lookup table.	<code>inputcsv</code> , <code>join</code> , <code>lookup</code> , <code>outputlookup</code>
<code>iplocation</code>	Extracts location information from IP addresses.	
<code>join</code>	Combine the results of a subsearch with the results of a main search.	<code>appendcols</code> , <code>lookup</code> , <code>selfjoin</code>
<code>kmeans</code>	Performs k-means clustering on selected fields.	<code>anomalies</code> , <code>anomalousvalue</code> , <code>cluster</code> , <code>outlier</code>
<code>kvform</code>	Extracts values from search results, using a form template.	<code>extract</code> , <code>kvform</code> , <code>multikv</code> , <code>xmlkv</code> , <code>rex</code>

<code>loadjob</code>	Loads events or results of a previously completed search job.	<code>inputcsv</code>
<code>localize</code>	Returns a list of the time ranges in which the search results were found.	<code>map, transaction</code>
<code>localop</code>	Run subsequent commands, that is all commands following this, locally and not on remote peers.	
<code>lookup</code>	Explicitly invokes field value lookups.	
<code>makecontinuous</code>	Makes a field that is supposed to be the x-axis continuous (invoked by chart/timechart)	<code>chart, timechart</code>
<code>makemv</code>	Change a specified field into a multivalued field during a search.	<code>mvcombine, mvexpand, nomv</code>
<code>makeresults</code>	Creates a specified number of empty search results.	
<code>map</code>	A looping operator, performs a search over each search result.	
<code>metadata</code>	Returns a list of source, sourcetypes, or hosts from a specified index or	<code>dbinspect</code>



	distributed search peer.	
<code>metasearch</code>	Retrieves event metadata from indexes based on terms in the logical expression.	<code>metadata</code> , <code>search</code>
<code>multikv</code>	Extracts field-values from table-formatted events.	
<code>multisearch</code>	Run multiple <b>streaming searches</b> at the same time.	<code>append</code> , <code>join</code>
<code>mvcombine</code>	Combines events in search results that have a single differing field value into one result with a multivalue field of the differing field.	<code>mvexpand</code> , <code>makemv</code> , <code>nomv</code>
<code>mvexpand</code>	Expands the values of a multivalue field into separate events for each value of the multivalue field.	<code>mvcombine</code> , <code>makemv</code> , <code>nomv</code>
<code>nomv</code>	Changes a specified multivalued field into a single-value field at search time.	<code>makemv</code> , <code>mvcombine</code> , <code>mvexpand</code>
<code>outlier</code>	Removes outlying numerical values.	<code>anomalies</code> , <code>anomalousvalue</code> , <code>cluster</code> , <code>kmeans</code>
<code>outputcsv</code>	Outputs search results to a specified CSV file.	<code>inputcsv</code> , <code>outputtext</code>

<code>outputlooku p</code>	Writes search results to the specified static lookup table.	<code>inputlookup</code> , <code>lookup</code> , <code>outputcsv</code> , <code>outputlookup</code>
<code>outputtext</code>	Outputs the raw text field ( <code>_raw</code> ) of results into the <code>_xml</code> field.	<code>outputtext</code>
<code>overlap</code>	Finds events in a summary index that overlap in time or have missed events.	<code>collect</code>
<code>pivot</code>	Run pivot searches against a particular data model object.	<code>dbinspect</code>
<code>predict</code>	Enables you to use time series algorithms to predict future values of fields.	<code>x11</code>
<code>rangemap</code>	Sets RANGE field to the name of the ranges that match.	
<code>rare</code>	Displays the least common values of a field.	<code>sirare</code> , <code>stats</code> , <code>top</code>
<code>regex</code>	Removes results that do not match the specified regular expression.	<code>rex</code> , <code>search</code>
<code>relevancy</code>	Calculates how well the event matches the query.	
<code>reltime</code>	Converts the difference between 'now' and ' <code>_time</code> ' to a	<code>convert</code>

	human-readable value and adds this value to the field, 'retime', in your search results.	
<code>rename</code>	Renames a specified field; wildcards can be used to specify multiple fields.	
<code>replace</code>	Replaces values of specified fields with a specified new value.	
<code>rest</code>	Access a REST endpoint and display the returned entities as search results.	
<code>return</code>	Specify the values to return from a subsearch.	<code>format, search</code>
<code>reverse</code>	Reverses the order of the results.	<code>head, sort, tail</code>
<code>rex</code>	Specify a Perl regular expression named groups to extract fields while you search.	<code>extract, kvform, multikv, xmlkv, regex</code>
<code>rtorder</code>	Buffers events from real-time search to emit them in ascending time order when possible.	
<code>savedsearch</code>	Returns the search results of a saved search.	

<code>script, run</code>	Runs an external Perl or Python script as part of your search.	
<code>scrub</code>	Anonymizes the search results.	
<code>search</code>	Searches indexes for matching events.	
<code>searchtxn</code>	Finds transaction events within specified search constraints.	<code>transaction</code>
<code>selfjoin</code>	Joins results with itself.	<code>join</code>
<code>sendemail</code>	Emails search results to a specified email address.	
<code>set</code>	Performs set operations (union, diff, intersect) on subsearches.	<code>append, appendcols, join, diff</code>
<code>setfields</code>	Sets the field values for all results to a common value.	<code>eval, fillnull, rename</code>
<code>sichart</code>	Summary indexing version of chart.	<code>chart, sitimechart, timechart</code>
<code>sirare</code>	Summary indexing version of rare.	<code>rare</code>
<code>sistats</code>	Summary indexing version of stats.	<code>stats</code>

<code>sitimechart</code>	Summary indexing version of timechart.	<code>chart</code> , <code>sichart</code> , <code>timechart</code>
<code>sitop</code>	Summary indexing version of top.	<code>top</code>
<code>sort</code>	Sorts search results by the specified fields.	<code>reverse</code>
<code>spath</code>	Provides a straightforward means for extracting fields from structured data formats, XML and JSON.	<code>xpath</code>
<code>stats</code>	Provides statistics, grouped optionally by fields. See also, <a href="#">Statistical and charting functions</a> .	<code>eventstats</code> , <code>top</code> , <code>rare</code>
<code>strcat</code>	Concatenates string values.	
<code>streamstats</code>	Adds summary statistics to all search results in a streaming manner.	<code>eventstats</code> , <code>stats</code>
<code>table</code>	Creates a table using the specified fields.	<code>fields</code>
<code>tags</code>	Annotates specified fields in your search results with tags.	<code>eval</code>
<code>tail</code>	Returns the last number n of specified results.	<code>head</code> , <code>reverse</code>

<code>timechart</code>	Create a time series chart and corresponding table of statistics. See also, <a href="#">Statistical and charting functions</a> .	<code>chart</code> , <code>bucket</code>
<code>top</code>	Displays the most common values of a field.	<code>rare</code> , <code>stats</code>
<code>transaction</code>	Groups search results into transactions.	
<code>transpose</code>	Reformats rows of search results as columns.	
<code>trendline</code>	Computes moving averages of fields.	<code>timechart</code>
<code>tscollect</code>	Writes results into tsidx file(s) for later use by <a href="#">tstats</a> command.	<code>collect</code> , <code>stats</code> , <code>tstats</code>
<code>tstats</code>	Calculates statistics over tsidx files created with the tscollect command.	<code>stats</code> , <code>tscollect</code>
<code>typeahead</code>	Returns typeahead information on a specified prefix.	
<code>typelearner</code>	Generates suggested eventtypes.	<code>typer</code>
<code>typer</code>	Calculates the eventtypes for the search results.	<code>typelearner</code>

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