**Important SPL Commands Quick Reference**

|  |  |  |  |
| --- | --- | --- | --- |
| **Command** | **Function** | **Example** | **Description** |
| search | Filters results based on search expression | | search product\_name = “Dream Crusher” | From the results, display events where product\_name is “Dream Crusher” |
| fields | Keeps or removes fields from the search results | | fields - count | Removes the field count from search results |
| rename | Rename fields | | rename count AS “Total Transactions” | Renames the filed count to “Total Transactions” |
| stats | Produces statistics from the search results | | stats avg(responseTime) | Calculates the average response time |
| timechart | Plots statistics with time in X axis | | timechart count | Plots the number of events over time |
| eval | Creates a new field based on an expression | | eval kb = bytes/1024 | Creates a new field kb by calculating bytes/1024 |
| dedup | Removes duplicate values | | dedup vendorId | Removes identical values of vendorId field |
| rex | Uses regular expressions to extract fields | | rex "(?<exception>java\.[^\s]+)" | Extracts java exceptions into a field named exception. |
| table | Returns a table with the fields you specify | | table host,source | Returns a table with the columns host and source from the search results |
| convert | Converts field values into specified numerical values | | convert ctime(\_indextime) AS IndexTime\_readable | Coverts the Unix Time value in \_indextime field into human readable form |
| metadata | Returns information about source,sourcetype and host from an index | | metadata type=hosts index=myIndex | Returns information like firstTime, lastTime and totalCount for the hosts in myIndex |
| where | Uses eval expressions to filter search results | | where avgheap > thereshold | Returns events where avgheap is more than threshold |
| append | Performs a subsearch and appends the results of into main search | | append [ search index=myIndex log\_level=FATAL ] | Appends results of the subsearch into main search |
| join | Merge results of a subsearch with main search based on join fields | | join host [ search index=myIndex] | Combines results from subsearch into the main search where the host field matches |
| head | Returns the first N number of events in search order | | head 15 | Returns the 15 most recent events |
| reverse | Reverses the order of the results | | reverse | Reverse the order of the results so the oldest data shows first |
| tail | Returns the last N number of events in search order | | tail 20 | Returns the 20 oldest events |
| top | Returns the most common values of the specified field | | top 5 host | Returns the top 5 hosts based on the number of events |
| transaction | Groups event based on constraints | | transaction JSESSIONID | Groups events by JSESSIONID |
| fillnull | Replaces null values with specified field | | fillnull value=”NA” | Replaces null values with the string “NA” |
| collect | Adds results to a summary index | | collect index=myStats | Stores the search results in an index named myStats |
| multikv | Extracts field values from table formatted events | | multikv fields pid command | From the search results, extract pid and command fields. |
| regex | Using regular expression removes results that do not match | | regex zip=”\d{5}” | Keeps only events with valid 5 digit zip code |
| lookup | Invokes field lookups on the specified lookup table | | lookup prices.csv productId | Retrieves column values from prices.csv where productId matches the event data |
| inputlookup | Retrieves the content of a lookup table | | inputlookup prices.csv | Display the contents of prices.csv |
| outputlookup | Write results to a lookup table | | outputlookup products.csv | Write search results to the lookup table products.csv |
| spath | Extracts fields from structured data such as JSON and XML | | spath output=message path=rec.log.msg | Extracts value from the JSON path rec.log.msg and writes to the field message |
| xmlkv | Extracts key-value pairs from XML data | | xmlkv | Creates key-value pairs from search results that are valid XML events |
| addtotals | Sums up all numerical fields in a search result and stores the total in a new field | | addtotals | Add all the numerical fields and store the result in the Total field. |
| tstats | Queries indexed fields and accelerated data models | | tstats count FROM datamodel=orders | Returns count from the data model orders. |