Cheatography

KQL Cheat Sheet

by Allyed via cheatography.com/175558/cs/36841/

Examples

Gather all logs sent by GA App	component : app
Gather all logs from GA App where the response wasn't 200	component : app and not responseCode : "200"
Gather all logs where the log level is ERROR	level : ERROR
Gather logs from a specific file	Source : "/logs/fuse.log"
Gather logs related to a specific correlation ID	correlationId : "5b1231cb-2e1d-4ae4-9d08-57ae8523ae2c"
Get an error log which didn't have a successful response code with a correlationId starting with '5b' or '4c' from the GA App	component : app and level : ERROR and not responseCode : "200" and correlationId : (5b* or 4c*)

Field Serach

Field Serach, e.g. component : app	Will return results that contain 'app' under the field named 'component'.
Field and Term OR, e.g. component : (app or solr)	Returns results containing either 'app' OR 'solr' under the field named 'component'.
Field and Term AND, e.g component : (app and solr)	Returns results containing 'app' AND 'solr' under the field named 'component'.
Exact Phrase Match, e.g. component : "solr dict 8"	Returns results where the words 'solr dict 8' are presented together under the field named 'component'.
Field Existance, e.g. component :* AND NOT component : app	Returns results with the field named 'component' but does not include results where the value 'app' exists.

Term Search

Keywords, e.g. Host Error	Will return results containing the words 'Host' and/or 'Error'.
Phrases, e.g "Host Error"	Returns results where the words 'Host Error' are present together.
OR Keyword, e.g. Host OR Error	Returns results where either the words 'Host' **or** 'Error' are present.
AND Keyword, e.g. Host AND Error	Returns results where the words 'Host' **and** 'Error' are both present.
Wildcard *, e.g. compo* : app or component : ap*	Asterisks are the only supported wildcards as of now, they can be used both in field names or in term values.

Range Search

Inclusive Range, e.g. [200 to 300]	Returns all values within the specified range including 200 and 300.
Exclusive Range, e.g. {200 to 300}	Returns all values within the specified range excluding 200 and 300.
Mathematical Equations, e.g. message_size\(in Byte\) >= 200	Returns any log where the 'message_size\(in Byte\)' field's value is greater than or equals 200 (works with <,>,<=,>=)

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com