Cheatography

Kibana Cheat Sheet

by spartan782 via cheatography.com/57408/cs/15187/

Terminology

Terminology	Description	Example
Term	A single word, subset of value	"term"
Phrase	A group of words inside quotes, subset of value	"this is a phrase"
Field	Is the name of the field that contains values. Appending a colon tells Lucene this is a Field	@meta.host:
Value	A value you wish to search	"this is a value or phrase"

Elastic Special Charactures

Characters	Description	Example
+ - && || ! () {} [] ^ " ~ * ? : \	These characters need to be escaped	"www.google.com/search\?source..."

Operators

Operator	Alternate Form	Description	Example
AND	&&	Only result that include both X AND Y	http AND www.google.com
OR	||	Only results that Include either X OR Y	http OR dns
NOT	!	Only results that do NOT include X	NOT ssl
TO		Results from value X to value Y	[10 TO 100]
+		X must be present in document text	+www.google.com
-		X must not be present in document text	-www.google.com
( )		Grouping of values, typically used to apply more advanced Boolean logic	http AND (get OR post)
[ ]		Inclusive range search, typically a number field but can search text. Will include specified values.	@meta.resp_port[1 TO 1024]
{ }		Exclusive range search, typically a number field but can search text. Will exclude specified values.	@meta.resp_port{0 TO 1025}
exists		Special operator that allows finding documents containing a specified field	_exists_: http.host
NOT _exists_		By combining the NOT operator you can find documents that are missing a field	NOT _exists_: http.user_agent

Field Searching

Field Search	Description	Example
field:value	The Colon states the previous text is a field and the text after it is the value you want to find	http.host:www.google.com
fiel\?:value	Wildcards be used inside a field name but need to be escaped	http.*:www.google.com

Cheatography

Kibana Cheat Sheet

by spartan782 via cheatography.com/57408/cs/15187/

Term Modifiers

Modifier	Description	Example
?	Single Character wildcard	www.googl?.com
*	Multiple Character wildcard	www.goo*.com
~	Fuzzy search based on Levenshtein distance	www.google.com~
~0.9	Change weight of fuzzy search, 0 to 1, default 0.5, higher number = Higher similarity	www.google.com~0.9
~2	Proximity search of values within # of each other	"program DOS"~10
^	Boost term to be more relevant in searches Default: 1, Must be Positive, can be decimal	"linux"^3

Lucene REGEX

REGEX	Description	Example	Matches
//	All regex starts and ends with a forward slash	/REGEX HERE/	
-	Range operator, a through z, 0 through 9	/[A-Z]/	Any single uppercase letter
.	Match any single character	/positv./	positv ending in anything
?	Preceding value is optional	/joh?n/	john or jon
+	Preceding value matched one or more times	/go+gle/	gogle with the o possibly repeating indefinitely
*	Preceding value matched zero or more times	/z*/	nothing or z possibly repeating indefinitely
|	Alteration operator, typically referred to as OR	/text|sms/	text or sms
[ ]	List, Matches one of the given expressions inside	/[abc123]/	a or b or c or 1 or 2 or 3
( )	Grouping, groups expressions together	/(([ab]) OR [12])/	a1 or a2 or b1 or b2
{ }	Intervals, repeat the preceding expression	/[ab]{1,3}/	ab or abab or abababab
\	Escape character	/[a\-z]/	a or - or z
"	Only needs escaped because its java regex		

By **spartan782**
cheatography.com/spartan782/

Not published yet.
Last updated 21st March, 2018.