Cheatography

Kibana Cheat Sheet

by swaglord via cheatography.com/30585/cs/9139/

Query

Match field	field1:"query_term"
Field contains A or B	field1:(term1 OR term2)
Field contains A and B	field1:(term1 AND term2)
Field missing	_missing_:field
Field exists	_exists_:title

Wilcards

Single character	?
Multiple characters	*
Fuzzy	~

Be careful with the * wildcard. It can create gigantic queries

Grouping

Basics (term operator term) operator term

Boolean logic combined with brackets
Example: Must contain either or both term1/term2 and term3
(term1 OR term2) AND term3

Boolean Operations

Must be Present	+
Must not be present	-
And	AND &&
or	OR ||
Not	NOT !

Ranges

1 to 5, including 1 and 5	[1 TO 5]
1 to 5, excluding 1 and 5	{ 1 TO 5 }
1 to 5, including 1, excluding 5	[1 to 5}
All days in 2012	[2012-01-01 TO 2012-12-31]
Larger then 3	>3
Smaller then 3	<3
Larger or equal to 3	>=3
Smaller or equal to 3	<=3

Reserved characters

Reserved	+ - = && || > < ! ( ) { } [ ] ^ " ~ * ? : \ /
Break character	\

For instance, to search for (1+1)=2, you would need to write your query as \(1\+1\)\=2

By **swaglord**
cheatography.com/swaglord/

Published 16th September, 2016.
Last updated 16th September, 2016.
Page 1 of 1.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com