Cheatography

Kibana Query Language (KQL) Cheat Sheet

by Sujit Ghosal (thesujit) via cheatography.com/210137/cs/45326/

Basic Queries

SYNTAX	DESC	EXAMPLE
Simple term	Search any field	*error*
Field value	Match exact field	*status:200*
Phrase	Match exact text	*message:"disk full"*
Field exists	Has any value	*status:**
Nested	Dot notation	*kubernetes.pod.name:nginx*

Comparisons

SYNTAX	DESC	EXAMPLE
>	Greater than	*bytes > 1000*
<	Less than	*status < 500*
>=	Greater/equal	*@timestamp >= "2023-01-01"*
<=	Less/equal	*response.time <= "2024-01-01"*

Wildcards

SYNTAX	DESC	EXAMPLE
*	Many chars	*user*name*
?	One char	*user?name*
Prefix	Starts with	*error**
Contains	Inside text	**error**
Suffix	Ends with	**.com*

Arrays

SYNTAX	DESC	EXAMPLE
Any match	Match array value	*tags:(error or warning)*
All match	All must match	*tags:(error and info)*
Exists	Has any value	*tags:**
Empty	No values	*not _exists_:tags*
Single match	One specif	*tags:error*
Exclude	Remove match	*not tags:error*

Boolean Logic

SYNTAX	DESC	EXAMPLE
AND	Both match	*status:200 and method:GET*
OR	Either matches	*status:(200 or 201)*
NOT	Negate	*not status:400*
Combined	Mix operators	*status:200 and (user:john or user:svc)*

Lists & Ranges

SYNTAX	DESC	EXAMPLE
Value list	Any match	*status:(200 or 201 or 204)*
Number range	Between values	*status >= 200 and status <= 299*
Date range	Time period	*@timestamp >= "now-24h"*
Multi-field	Match any field	*labels.(app:nginx or env:prod)*
Inclusive range	Include 1 and 10	*[1 to 10]*
Exclusive range	Exclude 1 and 10	*{1 to 10}*

Time Queries

SYNTAX	DESC	EXAMPLE
Now	Current time	*@timestamp >= now*
Relative	Time offset	*@timestamp > now-1h*
Calendar	Round to unit	*@timestamp >= now/d*
Time units	m, h, d, w, M, y	*@timestamp > now-7d*

Special Cases

SYNTAX	DESC	EXAMPLE
Null	Is null	*tags:null*
Boolean	True/false	*active:true*
IP	CIDR format	*ip:10.0.0.0/24*

By **Sujit Ghosal** (thesujit)
cheatography.com/thesujit/

Not published yet.
Last updated 24th December, 2024.