Kibana Cheat Sheet

Search Type	Example 1	Example 2
Keyword	WCESERVICE	
Phrase	"/WINDOWS/system32/config/"	
OR Keyword	WCESERVICE OR “WCE SERVICE”	WCESERVICE “WCE SERVICE”
AND Keyword	eo.oe.kiwi AND gentilkiwi.org	
NOT Keyword	NOT dropbox.com	
Must be present	“cmd.exe” +temp	
Must not be present	“cmd.exe” -”conhost.exe”	
Grouping	CommandLine:"cmd.exe" AND NOT (ParentCommandLine:nagios OR User:SYSTEM)	
Field Match	termname:keywordone	source_short:webhist
Exact Field Match	parser.raw:"sqlite/firefox_cookies"	
OR Term Search	source_short:(reg evt)	source_short:reg source_short:evt
Wildcard in Field	book.*:”quick brown”	
Field Exists	_exists_:star	
Field Missing	_missing_:star	
Wildcards	*.exe	url:*.ppt?
Regex[1]	/doc([mx]?)/	lang.raw:/e[ns]/
Fuzzy	svchost~	lsass~1
Proximity	”quick fox”~5	
Numeric Values	dport:>=1025	dport:8000
Range Search	code:[400 TO 599]	
OR on Fields	dport:(80 OR 443)	action:(Deny Reject)

Placeholder	Description	Example	Matches
?	Exactly one character	lang:e?	en, es
*	Any amount of chars (including 0)	port:80*	8080, 80, 888
~	Fuzzy search	sarah~	sarah, sahra, sara

Function	Command
_field	Internal Field
_all	The complete line (will be automatically prepended if no field is set)
.raw	The un-analyzed field value (case-sensitive; analyzed is case-insensitive)

[1] Not analyzed (.raw fields): Regex must match the whole value.
Analyzed fields: Regex must match a whole term and doesn't matches across multiple terms.

Elasticsearch Cheat Sheet

General	Example
Cluster Health	GET /_cluster/health?pretty GET /_cluster/health?wait_for_status=yellow&timeout=50s
Cluster State	GET /_cluster/stats?human&pretty
Pending Tasks	GET /_cluster/pending_tasks
Nodes	GET /_nodes
Node Stats	GET /_nodes/stats
Allocation	GET /_cat/allocation?pretty&v
List Indices	GET /_cat/indices/ GET /_cat/indices/*-2016.01.01
List Shards	GET /_cat/shards/?pretty&v

Search Type	Example
Search 1	GET /_search?q=dump
Search 2	GET /_search?q=EventCode:(512 OR 1102) AND NOT host:ImageServ*
Search with Date	GET /_search?q=message:hacker~3 AND date:[2016-01-01 TO 2018-12-31]
Get Aliases	GET /_aliases GET /myindex/_alias/* GET /*/_alias/*

Index Work	Request
Close Index (save resources)	POST /myindex /_close
Open Index	POST /myindex /_open
Index Monitoring	GET /myindex/_stats
Index Status and Management	POST /my_index_name/_cache/clear POST /my_index_name/_refresh POST /my_index_name/_flush POST /my_index_name/_forcemerge POST /my_index_name/_upgrade GET /my_index_name/_upgrade?pretty&human
Delete Index	DELETE /my_index_name DELETE/*-2016.01.*

Sources	URL
Kibana Search	https://www.timroes.de/2016/05/29/elasticsearch-kibana-queries-in-depth-tutorial/
Elastic Search	http://elasticsearch-cheatsheet.jolicode.com/
Basis Kibana	https://www.cheatography.com/maurermj08/cheat-sheets/kibana-search-tips/
Authors	@cyb3rops @blubbfiction