数象云日志查询语法Cheat Sheet

基本字符串	单引号字符串：'single quoted' 双引号字符串："double quoted" 反引号字符串：`back tick quoted` RE2 正则表达式：/.*mysql.*/ 或 /192\.168\.3\.\d{1,3}/	根据情况在过滤条件和下列函数参数中可使用单引号，双引号，反引号字符串或正则表达式
标签过滤函数	{label="value"} 或 {label!="value"} 或 {label ~ /regexp/} 或 {label !~ /regexp/} {level="warn" or level="error"} 或 {svc ~ /.*mysql.*/ and region !~ /.*asia.*/}	
	filter service="website" and category="prod" filter type=/.*mysql.*/ or server=/.*redis.*/	一个filter可以使用多个条件，用and或or组合起来 多个filter可以通过管道符号“|”串联起来达到同样效果
日志过滤函数	grep "include" grep -v "exclude" match "root" and not "exclude"	grep 支持对单个关键过滤 match可支持多个关键字通过and或or进行组合的过滤 可以通过管道符号“|”串联多个grep或match
标签扩充函数	json json label1=field1 field2	将所有json字段名扩展为标签，值为对应字段值 将字段field1扩展为标签label1，将field2扩展为同名标签
	pattern '<ip> <_> "<method> <uri>" <status> <size> <_>'	用模式匹配扩展标签，把（比如nginx）日志中对应的字段信息提取出来展开为标签，注意内容有引号是，酌情使用单引号，双引号或反引号定义模式
	regexp /POST (?P<uri>.*) .* (?P<code>\d+) (?P<size>\d+)/	用regexp进行模式提取，不需要全文匹配，只需对关心部分用regexp进行匹配后通过子匹配串，即(?P<name>re)定义所需扩展标签
	logfmt	将日志中的key=value对展开为标签
时序化日志	range auto use count range 5m use rate	用指定方法将日志流进行统计并转换为时序数据，转换时可指定步长为auto或具体的值，如30s，5m或1h
	range size 1m use rate range requests auto use sum	将指定标签的值当做**数值**并使用指定的方法按指定的步长进行处理后转换为时序数据。
时序归集处理	sum by (api, uri) count by client top 3 by api	对时序化的时序数据做进一步归集或聚合处理
显示设置	/as pie /as bars	仅适用于查询语法输出时序数据时，置于语句最后告诉系统如何展示处理好的时序数据。缺省将处理好的时序数据按线条进行展示。

详细语法请参考：https://www.zervice.cn/docs/manual/log/syntax/