# Kibana搜索语法

# 本课程仅用于教学用途

**中华人民共和国网络安全法**

**中华人民共和国刑法**

**社会主义核心价值观**

**详情百度搜索以上“关键词”+site:gov.cn**

# 目 录

# 一-参考资料

**Kibana指南**

**https://www.elastic.co/guide/en/kibana/current/index.html**

**Elasticsearch DSL语法**

**https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html**

# 二-关键词搜索

1~hello world　包含hello或者world或者hello world

2~"hello world"　包含hello world

3~response.body:hello world　返回包包含hello或者world或者hello world

4~response.body:(hello world)

5~response.body:"hello world"　返回包包含hello world

# 三-范围搜索

1~responsetime:>=190　大于等于190

2~responsetime:(>190 && <200)　大于190，小于200，记得空格

3~responsetime:{190 TO 200]　190到200之间，不含190，包含200

4~responsetime:[100 TO *]　一端不受限

5~@timestamp:["2019-12-25T12:00:00Z" TO "2019-12-25T23:59:59Z"]
2019年12月25号晚上20点到26号08点

6~unix_time:[1577203200 TO 1577246400]
2019.12.25 00:00:00到2019.12.25 12:00:00，需要进行时间戳的转换

7~@timestamp:{"now-1h" TO "now"}　　现在至1个小时之前的日志记录

# 四-逻辑运算搜索（上）

1~+request.host:www.pjzhang.com +realUrl:*login*
主机名www.pjzhang.com，url包含login

2~+request.host:www.pjzhang.com realUrl:*login*
主机名www.pjzhang.com，url可以包含login（可有可无）

3~+request.host:*pjzhang.com -request.host:www.pjzhang.com
4~request.host:(*pjzhang.com -www.pjzhang.com)
主机名包含pjzhang.com，但不能是www.pjzhang.com

5~request.host:(*pjzhang.com AND www.pjzhang.com)
6~request.host:(*pjzhang.com && www.pjzhang.com)
主机名www.pjzhang.com

# 四-逻辑运算搜索（下）

1~request.host:(*pjzhang.com NOT www.pjzhang.com)
2~request.host:(*pjzhang.com !www.pjzhang.com)
主机名包含pjzhang.com，但不能是www.pjzhang.com，叹号要和否定的内容相连

3~response.code:(200 || 301 || 404)
4~response.code:(200 | 301 | 404)
5~response.code:(200 OR 301 OR 404)
数字与竖线或者OR之间也需要空格

6~request.host:(www.pjzhang.com OR www.pjzhang.cn) AND response.code:200
主机名为www.pjzhang.com或者www.pjzhang.cn，响应码是200

# 五-通配转义正则搜索

1~realUrl:*login*　url包含login，*表示0个及以上个字符

2~realUrl:*sign?p*　?表示1个字符，例如signup

3~response*:200　含有response，且数值是200，转义符号也必不可缺少

4~request.content-type:text\/html
需要转义内容类型的值才可以查询，例如+ - = && || > < ! ( ) { } [ ] ^ " ~ * ? : \ /

5~request.host:/www\..*\.com/
开头是www，结尾是com的域名，需要在//中写入正则表达式，功能有限

6~response.body:/10\.(\d{1,3}\.){2}\d{1,3}/
查询返回包中含有内网IP的情形

# 六-模糊近似优先搜索

1~request.host:www.pjzhang.cn ~
2~request.host:www.pjzhang.cn ~1
模糊查询，结果中有www.Pjzhang.cn，~符号后面默认是2，设置为0的时候就是精确查询

3~"404 Found"~1
404 Found这个短语中间可以隔着1个单词，404和Found顺序可以调换

4~404^2 Found　　404出现的优先级高于Found，Found默认是1

5~404^0 Found　　404出现的优先级为0，表示不出现

# 软件工具

1. WPS演示
2. 迅捷屏幕录像工具
3. 爱奇艺视频助手

# 共勉

学好英语
早睡早起
少看手机
多多实践


感谢筒子们观看咯！