07 elastAlert实现ES日志告警

> 徐亮伟, 江湖人称标杆徐。多年互联网运维工作经验，曾负责过大规模集群架构自动化运维管理工作。擅长Web集群架构与自动化运维，曾负责国内某大型电商运维工作。
> 个人博客"徐亮伟架构师之路"累计受益数万人。

1.elastAlert安装

1.1 安装依赖包

```
[root@elast ~]# yum install git wget redhat-rpm-config gcc gcc-c++ libffi-devel python3-devel openssl openssl-devel -y
```

1.2 安装Python环境

```
[root@elast ~]# yum install python36 python36-devel python36-pip python36-cffi -y
[root@elast ~]# python3 -m pip install --upgrade pip
[root@elast ~]# python3 -m pip config set global.index-url https://mirrors.aliyun.com/pypi/simple/
```

1.3 下载elastAlert

```
# https://www.cnblogs.com/fatzi/p/13020824.html
[root@elast ~]# git clone https://github.com/Yelp/elastalert.git
[root@elast ~]# cd elastalert

#安装elastalert
[root@elast elastalert]# pip3 install "setuptools>=11.3"
[root@elast elastalert]# pip3 install "setuptools_rust"
[root@elast elastalert]# pip3 install "elasticsearch<7,>6"
[root@elast elastalert]# pip3 install -r requirements.txt
[root@elast elastalert]# python3 setup.py install
```

1.4 配置elastAlert

```
[root@elast elastalert]# vim config.yaml
# 用来加载rule的目录，默认是example_rules
rules_folder: example_rules

# 设置告警的频率，每1分钟执行一次告警
run_every:
  minutes: 1
  # seconds: 30
# 读取日志范围：读取最近1分钟的日志
buffer_time:
  minutes: 1

# 设置elasticsearch的地址及端口
es_host: 172.16.1.161
es_port: 9200


# elasticsearch的认证用户名+密码
#es_username: someusername
#es_password: somepassword

# 索引名称
writeback_index: elastalert_status
writeback_alias: elastalert_alerts

# 失败重试的时间限制
alert_time_limit:
  days: 2
```

1.5 创建elastAlert索引

```
[root@elast elastalert]# elastalert-create-index --config config.yaml
Elastic Version: 7.8.1
Reading Elastic 6 index mappings:
Reading index mapping 'es_mappings/6/silence.json'
Reading index mapping 'es_mappings/6/elastalert_status.json'
Reading index mapping 'es_mappings/6/elastalert.json'
Reading index mapping 'es_mappings/6/past_elastalert.json'
Reading index mapping 'es_mappings/6/elastalert_error.json'
New index elastalert_status created
Done!
```

1.6 测试告警是否正常

```
[root@elast elastalert]# # python3 -m elastalert.elastalert --verbose --config config.yaml --rule ./example_rules/example_spike.yaml
```

1.7 elastAlert集成钉钉

```
[root@elast elastalert]# git clone https://github.com/xuyaoqiang/elastalert-dingtalk-plugin.git
# 解压的方式
[root@logstash-node1 ~]# unzip elastalert-dingtalk-plugin.zip
[root@elast elastalert]# cd elastalert-dingtalk-plugin-master
[root@elast elastalert]# cp -rp elastalert_modules/ /root/elastalert
```

2.请求频繁出现404-场景1

2.1 编写告警规则

```
[root@elast elastalert]# cat /root/elastalert/example_rules/nginx_404.yaml
# 告警名称
name: nginx_access_404

# 告警类型
type: frequency

# 告警匹配的索引名称
index: kafka-nginx-access*

#告警的条件，查询最近1分钟的日志，当10s内发生5次404错误则触发告警

```

```
num_events: 5
timeframe:
  seconds: 10
  #minutes: 1

filter:
- query:
    query_string:
      query: "response: 404"


# 告警方式：钉钉
alert_text_type: alert_text_only
alert:
- "elastalert_modules.dingtalk_alert.DingTalkAlerter"
dingtalk_webhook: "https://oapi.dingtalk.com/robot/send?access_token=e27d9d952d5b2c3eab48a8f2a1217766569361020c4dba60f0372e98af2728c5"
dingtalk_msgtype: "text"

alert_text: |
  告警程序：ElasticSearch_Alert
  告警节点：{}
  域      名：{}
  调用方式：{}
  请求链接：{}
  触发条件：10s 内 {} 状态码 超过 {} 次
```

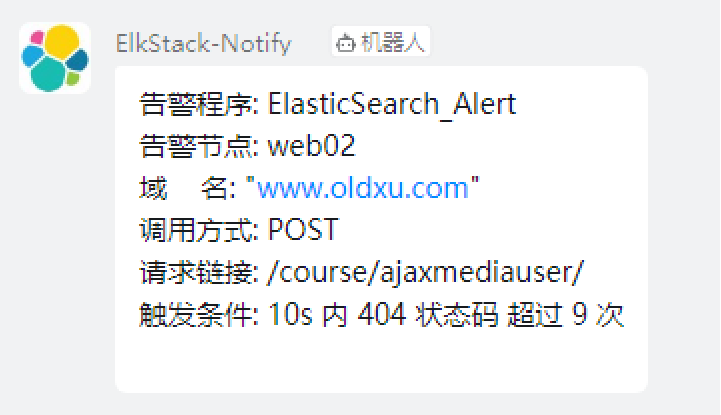
```
alert_text_args:
  - host.name
  - hostname
  - method
  - request
  - response
  - num_hits
```

2.2 执行告警规则

```
[root@web ~]# cd elastalert
[root@web ~]# python3 -m
elastalert.elastalert --verbose --config
config.yaml --rule
./example_rules/nginx_404.yaml
```

2.3 测试告警规则

测试钉钉告警： 模拟产生404日志，通过追加对应时间点的日志即可完成测试；



告警程序: ElasticSearch_Alert
告警节点: web02
域　名: "www.oldxu.com"
调用方式: POST
请求链接: /course/ajaxmediauser/
触发条件: 10s 内 404 状态码 超过 9 次

```
[root@web ~]# echo '14.145.74.175 - -
[01/Nov/2021:17:05:06 +0800] "POST
/course/ajaxmediauser/ HTTP/1.1" 404 54
"www.oldxu.com"
"http://www.oldxu.com/video/678"
mid=678&time=60&learn_time=551.5
"Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/45.0.2454.101 Safari/537.36" "-"
10.100.136.64:80 200 0.014 0.014' >>
/var/log/nginx/access.log
```

3.请求频繁出现500-场景2

3.1 编写告警规则

```
[root@elast elastalert]# cat
/root/elastalert/example_rules/nginx_5xx.yaml
# 告警名称
name: nginx_access_5xx

# 告警类型
type: frequency

# 告警匹配的索引名称
index: kafka-nginx-access*

```

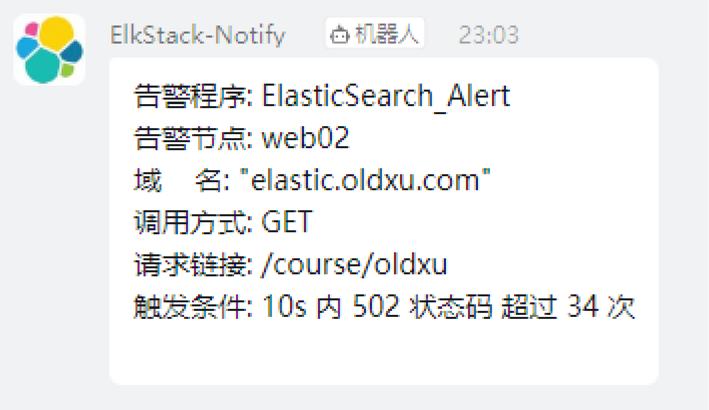
```
#告警的条件，查询最近1分钟的日志，当10s内发生5次500-509错误则触发告警
num_events: 5
timeframe:
  seconds: 10
  #minutes: 1

filter:
- query:
    query_string:
      query: "response: [500 TO 599]"


# 告警方式：钉钉
alert_text_type: alert_text_only
alert:
- "elastalert_modules.dingtalk_alert.DingTalkAlerter"
dingtalk_webhook: "https://oapi.dingtalk.com/robot/send?access_token=e27d9d952d5b2c3eab48a8f2a1217766569361020c4dba60f0372e98af2728c5"
dingtalk_msgtype: "text"

alert_text: |
  告警程序: ElasticSearch_Alert
  告警节点: {}
  域    名: {}
  调用方式: {}
  请求链接: {}
  触发条件: 10s 内 {} 状态码 超过 {} 次

alert_text_args:
  - host.name
  - hostname
  - method
  - request
  - response
  - num_hits
```

3.2 执行告警规则

```
[root@elast elastalert]# python3 -m elastalert.elastalert --verbose --config config.yaml --rule example_rules/nginx_5xx.yaml
```

3.3 测试告警规则

测试钉钉告警： 模拟产生500日志，通过追加对应时间点的日志即可完成测试；



告警程序: ElasticSearch_Alert
告警节点: web02
域　名: "elastic.oldxu.com"
调用方式: GET
请求链接: /course/oldxu
触发条件: 10s 内 502 状态码 超过 34 次

```
[root@web ~]# echo '14.145.74.175 - -
[01/Nov/2021:17:09:06 +0800] "GET
/course/oldxu HTTP/1.1" 502 54
"elastic.oldxu.com"
"http://www.oldxu.com/video/678"
mid=678&time=60&learn_time=551.5
"Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/45.0.2454.101 Safari/537.36" "-"
10.100.136.64:80 200 0.014 0.014' >>
/var/log/nginx/access.log
```

4.请求url超过3秒则-场景3

4.1 编写告警规则

```
[root@elast elastalert]# cat
/root/elastalert/example_rules/nginx_respon
se.yaml
# 告警名称
name: nginx_response_time
```

```
# 告警类型
type: frequency

# 告警匹配的索引名称
index: kafka-nginx-access*

#告警的条件，查询最近1分钟的日志，当10s内发生5次响应超过3s
num_events: 5
timeframe:
  seconds: 10
  #minutes: 1

filter:
filter:
- query_string:
    query: "response_time: >3"


# 告警方式：钉钉
alert_text_type: alert_text_only
alert:
- "elastalert_modules.dingtalk_alert.DingTalkAlerter"
dingtalk_webhook: "https://oapi.dingtalk.com/robot/send?access_token=e27d9d952d5b2c3eab48a8f2a1217766569361020c4dba60f0372e98af2728c5"
```

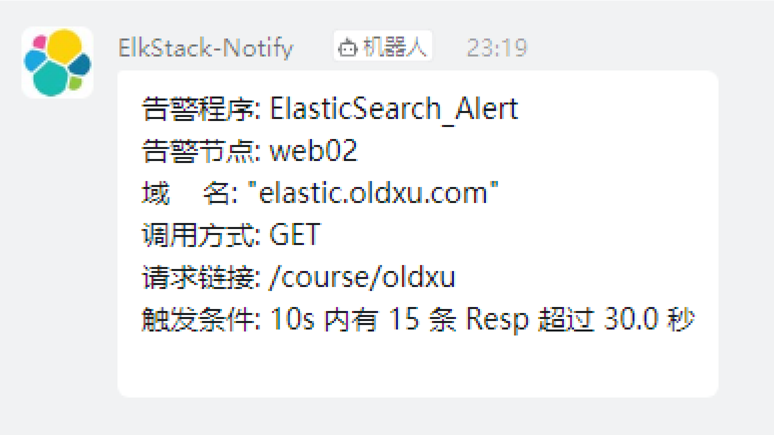
```
dingtalk_msgtype: "text"

alert_text: |
  告警程序: ElasticSearch_Alert
  告警节点: {}
  域    名: {}
  调用方式: {}
  请求链接: {}
  触发条件: 10s 内有 {} 条 Resp 超过 {} 秒

alert_text_args:
  - host.name
  - hostname
  - method
  - request
  - num_hits
  - response_time
```

4.2 执行告警规则

```
[root@elast elastalert]# python3 -m
elastalert.elastalert --verbose --config
config.yaml --rule
example_rules/nginx_response.yaml
```

4.3 测试告警规则

测试钉钉告警： 模拟response大于3s的日志，通过追加对应时间点的日志即可完成测试；



告警程序: ElasticSearch_Alert
告警节点: web02
域　名: "elastic.oldxu.com"
调用方式: GET
请求链接: /course/oldxu
触发条件: 10s 内有 15 条 Resp 超过 30.0 秒

```
[root@web ~]# echo '14.145.74.175 - -
[01/Nov/2021:17:13:06 +0800] "GET
/mp3/oldxu HTTP/1.1" 200 54
"elastic.oldxu.com"
"http://www.oldxu.com/video/678"
mid=678&time=60&learn_time=551.5
"Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/45.0.2454.101 Safari/537.36" "-"
10.100.136.64:80 200 0.014 30' >>
/var/log/nginx/access.log
```