> https://elastalert.readthedocs.io/en/latest/running_elastalert.html

安装步骤

安装软件

```
# 环境软件安装
yum install gcc
yum install libffi-devel
yum install python-devel
# elastalert安装
pip install elastalert
pip install "elasticsearch>=5.0.0"
```

配置config.yaml

```
#存放elastalert 规则的文件夹，你的elastalert 放到哪里就放到哪里就行了
# This is the folder that contains the rule yaml files
# Any .yaml file will be loaded as a rule
rules_folder: /usr/local/elastalert/example_rules

#Elastalert 多久去查询一下根据定义的规则去elasticsearch 查询是否有符合规则的字段，如果有就会触发报警，如果没有就等待下一次时间再检查，时间定义的单位从周到秒都可以，具体定义方法如下。
# How often ElastAlert will query Elasticsearch
# The unit can be anything from weeks to seconds
run_every:
  #seconds: 1
  minutes: 1
  #hours: 1
  #days: 1
  #weeks: 1

#当查询开始一直到结束，最大的缓存时间。
# ElastAlert will buffer results from the most recent
# period of time, in case some log sources are not in real time
buffer_time:
  minutes: 15

#你的Elasticsearch ip地址
# The Elasticsearch hostname for metadata writeback
# Note that every rule can have its own Elasticsearch host
es_host: 192.168.115.65

```

```
#Elasticsearch 的端口
# The Elasticsearch port
es_port: 9200

#是不是用TLS 加密
# Connect with TLS to Elasticsearch
#use_ssl: True

#是不是启动TLS证书验证
# Verify TLS certificates
#verify_certs: True

#如果Elasticsearch 有认证的话需要把这个填写上
# Option basic-auth username and password for Elasticsearch
#es_username: someusername
#es_password: somepassword

#配置证书存放的位置
# Use SSL authentication with client certificates client_cert must be
# a pem file containing both cert and key for client
#verify_certs: True
#ca_certs: /path/to/cacert.pem
#client_cert: /path/to/client_cert.pem
#client_key: /path/to/client_key.key

#这个是elastalert 在es里边写的index
# The index on es_host which is used for metadata storage
# This can be a unmapped index, but it is recommended that you run
# elastalert-create-index to set a mapping
writeback_index: elastalert_status

#如果alert当时没有发出去重试多久之后放弃发送;
# If an alert fails for some reason, ElastAlert will retry
# sending the alert until this time period has elapsed
alert_time_limit:
  days: 2
```

添加rule 类型

```
“Match where there are X events in Y time” (frequency type)
“Match when the rate of events increases or decreases” (spike type)
```

```
“Match when there are less than X events in Y time” (flatline type)
“Match when a certain field matches a blacklist/whitelist” (blacklist and whitelist type)
“Match on any event matching a given filter” (any type)
“Match when a field has two different values within some time” (change type)
```

在es中添加elastalert index

```
elastalert-create-index
```

测试与运行

测试规则

```
elastalert-test-rule --config <path-to-config-file> example_rules/example_frequency.yaml
```

运行规则

```
python -m elastalert.elastalert --verbose --rule example_frequency.yaml
```

安装遇到错误

No local packages or working download links found for thehive4py>=1.4.4

```
pip install thehive4py
```

error: six 1.9.0 is installed but six>=1.10.0 is required by set(['jira'])

```
pip install --upgrade six
```

error: cryptography 1.7.2 is installed but cryptography>=2.3 is required by set(['pyOpenSSL'])

```
pip install --upgrade cryptography
```