ES Alert

简介

es-alert是基于Python编写的ES告警脚本，用于监控ES集群。

实现

主要组件

- application.py 程序入口，用于启动定时任务，检测ES集群状态
- es_alert.py 对ES集群进行监测，并产生告警
- es_request 请求es，解析结果
- alert_message 调用webhook，发送异常消息

流程图

- ES集群告警流程：https://www.kdocs.cn/view/p/151536032998
- ES集群告警流程V2：https://www.kdocs.cn/view/p/151536112808

配置文件

```
elasticsearch:
  hosts: ["127.0.0.1"]
  port: 9200
  user:
  password:
kibana:
  url: "http://127.0.0.1:5601"
woa:
  webhook: "https://woa.wps.cn/api/v1/webhook/send?
key=28d081506cf36e698bae832d8e048ec4"
```

> elasticsearch用于连接ES集群, woa用于消息通知, kibana用于查询ES集群异常日志

部署

安装依赖

```
pip install -r requirements.txt
```

执行脚本

```
sudo bin/startup.sh
```

本地开发

部署单节点ES集群

```
docker-compose -f docker/elasticsearch.yml up
```

部署3节点ES集群

```
docker-compose -f docker/elasticsearch-cluster.yml up
```

> 如果启动失败，则需要调整系统的最大文件数量 参考https://blog.csdn.net/Pointer_v/article/details/112395425

本地测试

场景1：单节点集群，索引副本大于1，自动愈合

描述：单节点集群，创建`blogs`索引，设置副本数为1。由于只有一个节点，所以会分配给主分片，副本分片无法分配，ES集群状态为yellow。

预期：通过es-alert检测集群状态，发出告警功能，通过修改`blogs`索引副本数为0，自动愈合，正常后发出通知。

实验步骤：

- 启动容器：docker-compose -f docker/elasticsearch.yml up
- 新建索引，并设置`blogs`索引副本数为1
- 启动es-alert服务

设置副本的脚本：

```
PUT /blogs/_settings
{
  "index" : {
    "number_of_replicas" : 1
  }
}
```

场景2：模拟`too many open files`异常，并产生告警

描述：单节点集群，模拟`too many open files`异常，并产生告警

实验步骤：

1. 修改elasticsearch.yml中文件描述符数量：

```
    ulimits:
      nofile:
        soft: 1000
        hard: 1000
```

2. 批量写入1000条数据

```
curl -XPOST localhost:9200/blogs/_bulk --data-binary
@./test/bulk_insert_1000.txt
```

3. 查看es集群状态，出现`too many open files`异常

场景3：模拟`retries [5] on failed allocation attempts`异常，并产生告警

描述：对于ES集群中`retries [5] on failed allocation attempts`异常，执行reroute操作，并发送告警

TODO

- [ ] 添加更多ES自我愈合的场景
- [ ] 编写测试用例
- [ ] 基于namespace支持ES多集群