链滴

fluend+kibana 服务部署

作者：qifu
原文链接：https://ld246.com/article/1605866491732
来源网站：链滴

所有组件的时区保持一致并设置为东八区

由于fluentd和kibana需要依赖elasticsearch，所以elasticsearch要先启动

Fluentd部署(非HA部署)

创建配置文件

vi /data/fluent.conf

```
<source>
@type tail #读取日志文件
@label @whhconvergency
path /######/*.log   ### 要读取的日志文件路径
pos_file /fluent-pos/td-agent-whh/log.pos
tag whhconvergency
<parse>
  @type json
  <pattern>
    format json
    time_key time
    time_format %Y-%m-%dT%H:%M:%S.%NZ
  </pattern>
<pattern>
  format /^(?<time>.+) (?<stream>stdout|stderr) [^ ]* (?<log>.*)$/
  time_format %Y-%m-%dT%H:%M:%S.%N%:z
</pattern>
</parse>
</source>


<source>
@type tail
@label @ztconvergency
path /######/*.log
pos_file /fluent-pos/td-agent-zhongtai/log.pos
tag zhongtaiconvergency
<parse>
  @type json
  <pattern>
    format json
    time_key time
    time_format %Y-%m-%dT%H:%M:%S.%NZ
  </pattern>
<pattern>
  format /^(?<time>.+) (?<stream>stdout|stderr) [^ ]* (?<log>.*)$/
  time_format %Y-%m-%dT%H:%M:%S.%N%:z
</pattern>
</parse>
</source>

<label @whhconvergency>
<match *whh*>
```

原文链接：fluend+kibana 服务部署

```
@type elasticsearch
host #####
port 9200
logstash_format true
logstash_prefix whhfluentd
logstash_dateformat %Y%m%d
include_tag_key true
type_name access_log
tag_key @log_name
flush_interval 1s
</match>
</label>

<label @ztconvergency>
<match *zhongtai*>
@type elasticsearch
host #####
port 9200
logstash_format true
logstash_prefix zhongtaifluentd
logstash_dateformat %Y%m%d
include_tag_key true
type_name access_log
tag_key @log_name
flush_interval 1s
reload_connections false
reconnect_on_error true
reload_on_failure true
<buffer>
    @type file
    path /fluent-pos/log/elastic-buffer-zhongtai
    flush_thread_count 4
    flush_interval 1s
    chunk_limit_size 64M
    queue_limit_length 512
    flush_mode interval
    retry_max_interval 30
    retry_forever true
  </buffer>
</match>
</label>


<source>
  @type  tail #读取日志文件
  @id    lixingjia.log
  path /fluentd/etc/*.log ### 要读取的日志文件路径
  pos_file /fluentd/etc/td-agent/log.pos #读取的偏移值记录文件，可以提前创建一个空文件
  tag lxjtest
  <parse>                          # 多行格式化成JSON
    @type json
    <pattern>
      format json                   # JSON解析器
      time_key time                   # 指定事件时间的时间字段
```

```
    time_format %Y-%m-%dT%H:%M:%S.%NZ   # 时间格式
   </pattern>
   <pattern>
    format /^(?<time>.+) (?<stream>stdout|stderr) [^ ]* (?<log>.*)$/
    time_format %Y-%m-%dT%H:%M:%S.%N%:z
   </pattern>
  </parse>
</source>


<match **>
 @type elasticsearch  # 将结果输出到ES
 host   ####### es地址,要根据实际情况自己设置
 port 9200           #### es端口，要根据实际情况自己设置
 logstash_format true   # 格式化
 logstash_prefix Fluentd  #######推送到kibana的名称，根据这个名称做索引，建议使用客户+
目名称
 logstash_dateformat %Y%m%d
 include_tag_key true
 type_name access_log
 tag_key @log_name
 flush_interval 1s
</match>
```

上述模板使用的读取方式是直接使用tail模式进行日志文件读取，如需使用其他方式读取请参照fluent官方文档编写conf文件

如果使用直接读取日志的模式部署，fluentd要部署到可访问日志文件的机子上，如果日志文件在宿机上同时还需要将路径映射到容器内，fluentd.conf需要配置是容器内的日志路径，如下/fluent-dat下为要读取的日志文件路径，/fluent-pos用来存储偏移

下载该镜像需要进行docker仓库登录

docker login --username=100000541665 ccr.ccs.tencentyun.com

创建容器

```
docker create --network host --name fluentd -v /data/fluent.conf:/fluentd/etc/fluent.conf -v  /
luent-data:/fluent-data:ro -v  /fluent-pos:/fluent-pos -v /etc/localtime:/etc/localtime  --restart
always ccr.ccs.tencentyun.com/ceshi123buzhidaoqushenmemingzi/fluentd:1.3.2
```

启动容器

```
docker start fluentd
```

Kibana部署(非HA部署，镜像要与es一致)

创建配置文件

vi /data/kibana.yml

```
server.name: kibana
server.host: "0"
elasticsearch.hosts: [ "http://es的ip:es的port" ]
xpack.monitoring.ui.container.elasticsearch.enabled: true
i18n.locale: "zh-CN"
```

创建容器

```
docker create --network host --name kibana  -v /etc/localtime:/etc/localtime  -v /data/kibana yml:/usr/share/kibana/config/kibana.yml --restart always docker.elastic.co/kibana/kibana:7.8.0
```

启动容器

```
docker start kibana
```

=在中台2.11.X版本已输出日志为json格式,以下代码段为案例模板=


```
{
  "_index": "lxjfluentd-20200713",
  "_type": "_doc",
  "_id": "ccsLRnMBZGQN8A54wD5g",
  "_version": 1,
  "_score": null,
  "_source": {
    "date": "2020-07-13 10:40:39.948",
    "level": "INFO",
    "uin": "",
    "clientId": "",
    "deviceId": "",
    "traceId": "",
    "thread": "lettuce-eventExecutorLoop-1-1",
    "fileLine": "AbstractInternalLogger.java:171",
    "msg": "Reconnecting, last destination was 192.168.8.90:31791",
    "@timestamp": "2020-07-13T02:40:40.021660506+00:00",
    "@log_name": "lxjtest"
  },
  "fields": {
    "@timestamp": [
      "2020-07-13T02:40:40.021Z"
    ]
  },
  "sort": [
    1594608040021
  ]
}
```


创建Kibana的可视化面板

创建日志可视化直方图创建案例

1.创建直方图

2.指标：Y轴使用聚合：计数模式

3.在存储桶中新建一个X轴，选择聚合:词 ，选择level.keyword，排序依据选择指标：计数，定制标填写Log_Level。点击生成即可生成日志统计数直方图。点击左上角的保存将该可视化保存。

创建dashboard面板

一般是将多个可视化面板组合，直接选择已创建好的可视化面板进行组合即可。

[其他更多的功能组合请参考Kibana官方文档](https://www.elastic.co/guide/en/elasticsearch/reference/7.6/search-aggregations-bucket-terms-aggregation.html)