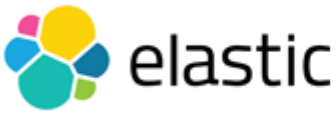
ELK应用之一卡易日志分析平台

夏小成

2016-09-10



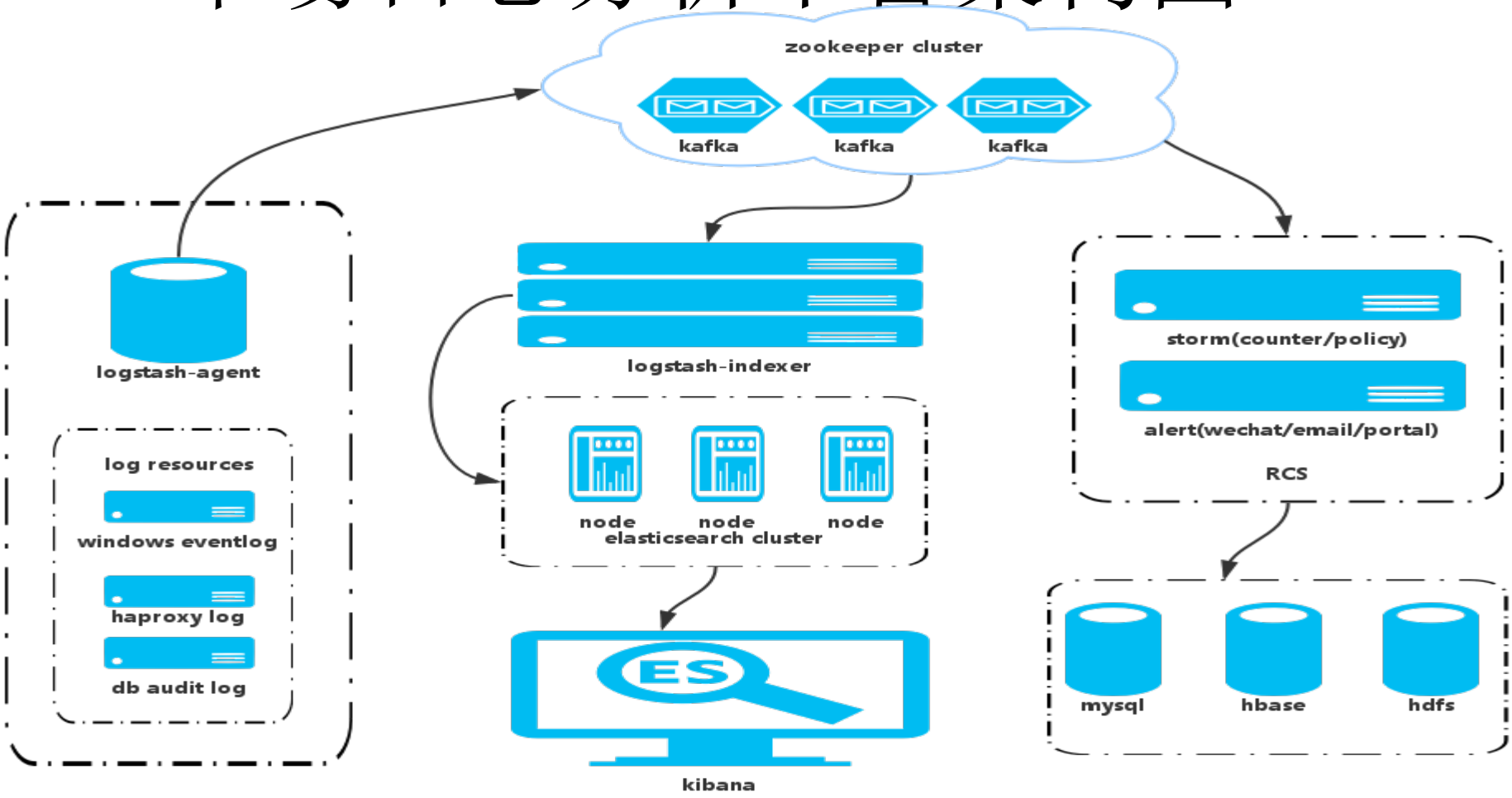
关于一卡易

- 企业级SaaS平台
- 专注会员营销、O2O和移动支付领域
- 新三板上市公司

一卡易架构现状

- windows/.net体系为主
- linux为辅
- 同时在往服务化过渡
- 大数据领域也在不断探索

一卡易日志分析平台架构图



一卡易日志平台动态

1、elasticsearch：2台物理机　26G内存 + 12核CPU
2、logstash-indexer: 1台虚拟机 12G内存 + 4核CPU
3、kibana: 1台虚拟机 8G内存 + 4核CPU
4、承载30G/天的日志量
5、日志平台目前支撑着100余台服务器

Logstash-agent 配置——windows

- **windows-shipper.conf**

```
input {
    eventlog {
        type = >'EventLog'logfile = >'Application'
    }
    output {
        kafka {
            topic_id = >"winlog"broker_list = >"10.10.13.15:9092"
        }
      }
    }
```

Logstash-agent 配置——linux

```
input {
   file {
      type = >"haproxy202"path = >"/var/log/haproxy.log"
   }
   file {
      type = >"haproxyerror202"path = >"/var/log/haproxy_error.log"
   }
}
output {
   kafka {
      topic_id = >"haproxy"bootstrap_servers = >"10.10.13.15:9092"#message_key
= >"whatis-key"workers = >2
   }
}
```

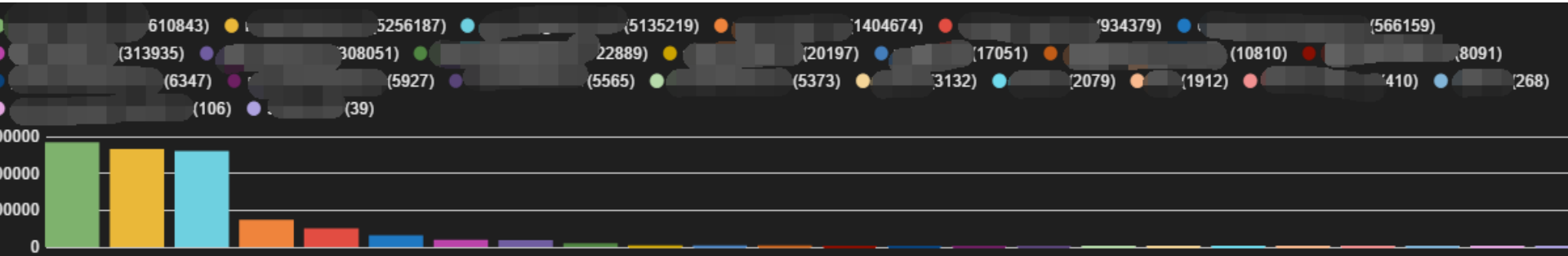
Logstash-indexer配置

```
filter {
  grok {
    match = >{
      "message" = >"%{HAPROXYHTTP}"
    }
    match = >{
      "message" = >"%{HAPROXYSP}"
    }
    match = >{
      "message" = >"%{HAPROXYTCP}"
    }
  }
  date {
    match = >["syslog_timestamp", "MMM dd HH:mm:ss", "MMM  d HH:mm:ss"]
  }
  geoip {
    source = >"client_ip"
  }
}
```

Haproxy日志解析正则

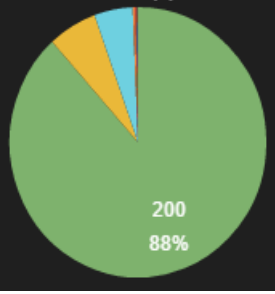
```
grok {
match => { "message" => "%{HAPROXYHTTP}" }
match => { "message" => "%{HAPROXYSP}" }
match => { "message" => "%{HAPROXYTCP}" }
}
```

grok中定义haproxy中3个变量%{HAPROXYHTTP}；%{HAPROXYSP};%{HAPROXYTCP}里面是正则匹配的，变量定义在/usr/local/logstash-2.2.0/vendor/bundle/jruby/1.9/gems/logstash-patterns-core-2.0.2/patterns/haproxy文件中



TP_STATUS_CODE

200 (17439271) 304 (1214388)
302 (955943) 404 (62310)
210 (31155) -1 (8157) 220 (5581)
500 (5218) 405 (5152) 206 (3735)
211 (3339) 503 (2211) 504 (1291)
403 (1214) 400 (319) 401 (156)
408 (119) 212 (44) 416 (20)
412 (12) 303 (4) 301 (2) 406 (1)
0 (1) Other values (0)



AVERAGE OF TR

231.426
ms (mean)

TR	max
*	188709.000 ms

AVERAGE OF TQ

1319.490
ms (mean)

tq	max	mean
*	63860.000 ms	1319.490 ms

AVERAGE OF TT

1558.500
ms (mean)

tt	max	mean
*	196119.000 ms	1558.500 ms

使用ELK的体会

- 1、简单快速接入、整体日志解决方案、提升定位分析的效率、低成本运维、活跃的社区
- 2、虚拟机换成物理机，并将队列由redis换成kafka
- 3、尝试将elasticsearch往业务迁移
- 4、结合大数据做进一步的探索

Thanks

elastic

VMC | vivo 移动互联网

Elastic中文社区技术沙龙【深圳站】

http://elastic.co

http://elasticsearch.cn

http://elasticsearch.cn/article/99

http://www.vivo.com.cn

http://dev.vivo.com.cn

http://hr.vivo.com.cn

http://www.vivo.com