GZLUG 5月份线下聚会

基于 KIBANA+LOGSTASH+ELASTICSEARCH 构建中央日志系统

2013年5月25日

夜行人@mingchao.com

About me

- 夜行人
- WebGame运维
- 参与游戏项目：六界先尊、仙落凡尘、明朝传奇、明朝时代
- 微信：153467301

Agenda

- 为什么要集中管理？
- 中央日志系统架构
- 收集PHP日志
- Kibana使用
- 存在问题

为什么要集中管理

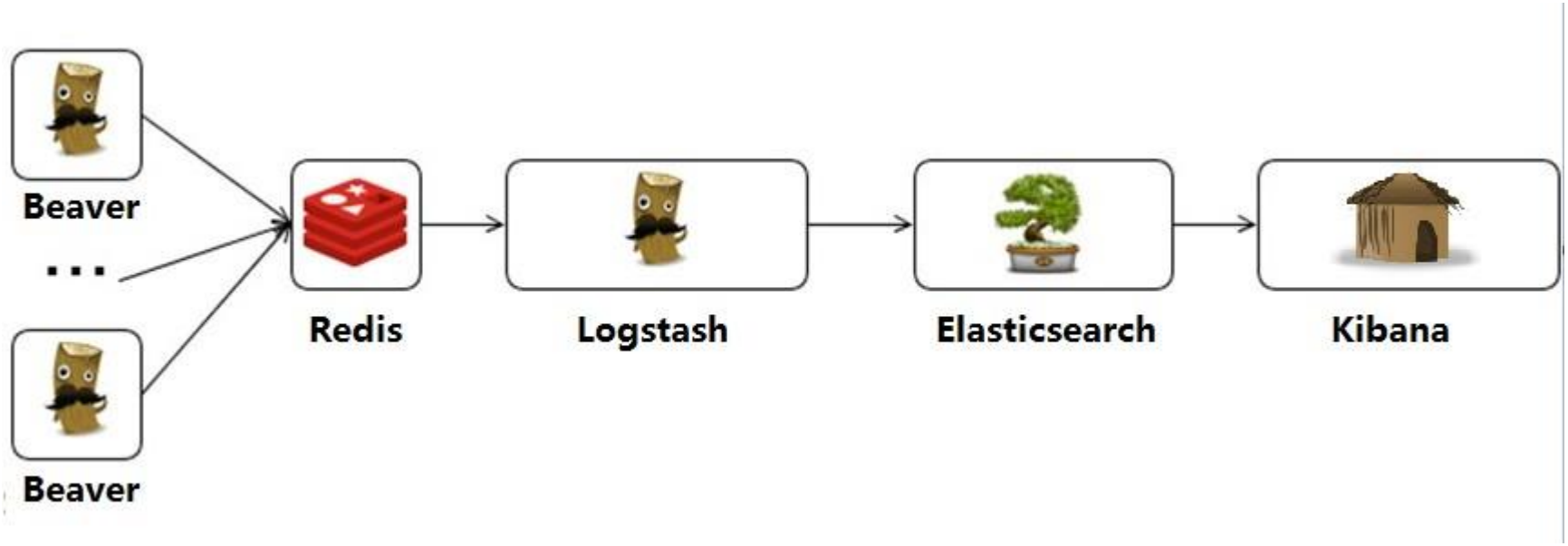
- 机器多，出问题就ssh去查
- 日志是集群里哪台机，哪个文件输出的？
- 出问题才查日志？让我们反过来，根据日志来报警

中央日志系统架构

- Logstash
  - input：redis、udpport(514)、file
  - filter：grok、grep、urldecode
  - output：elasticsearch、nagios、gtalk
  - 处理条件：type、tags、content
- Elasticsearch
  - 分布式，多台机组成集群
  - RESTful，通过HTTP的GET查询，POST添加数据，DELETE删除数据

- Kibana
  - Web search interface
- Redis
  - Broker
- Beaver
  - Log shipper
- Supervisor
  - Daemon management

架构图



收集PHP日志

- Beaver配置
- Logstash配置
- GROK正则

Beaver配置

[beaver]

redis_url: redis://localhost:6379/0

redis_namespace: logstash:web

redis_password: xxxxxxxxxxxx

[/var/log/php_error.log]

type: php

tags: web,php

beaver -c /data/conf/beaver/beaver.ini -t redis

Logstash配置

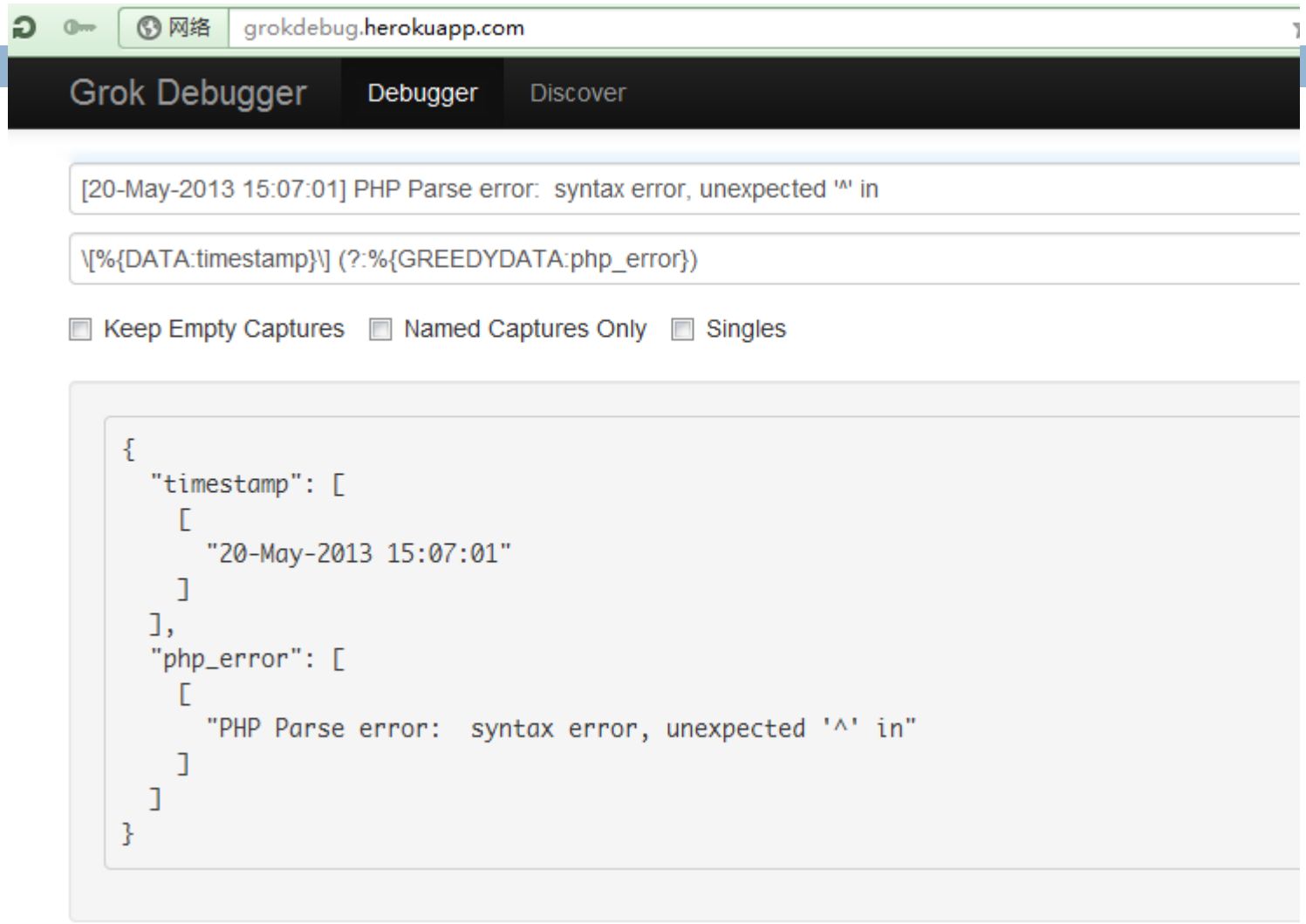
```
input
{
    redis
    {
        host => "127.0.0.1"
        password => "xxxxxxxxxxx"
        key => "logstash:web"
        type => "web"
        format => "json_event"
        data_type => "list"
    }
}
```

```
filter
{
    grok
    {
      tags => "php"
      pattern => "%{PHPLOG}"
      patterns_dir => ["/data/central_log/logstash/etc/patterns"]
    }

    grep
    {
       tags => "php"
       drop => "false"
       add_tag => ['error_alert']
       match => [ "@message","(syntax|ERROR|CRITICAL)" ]
    }
}
```

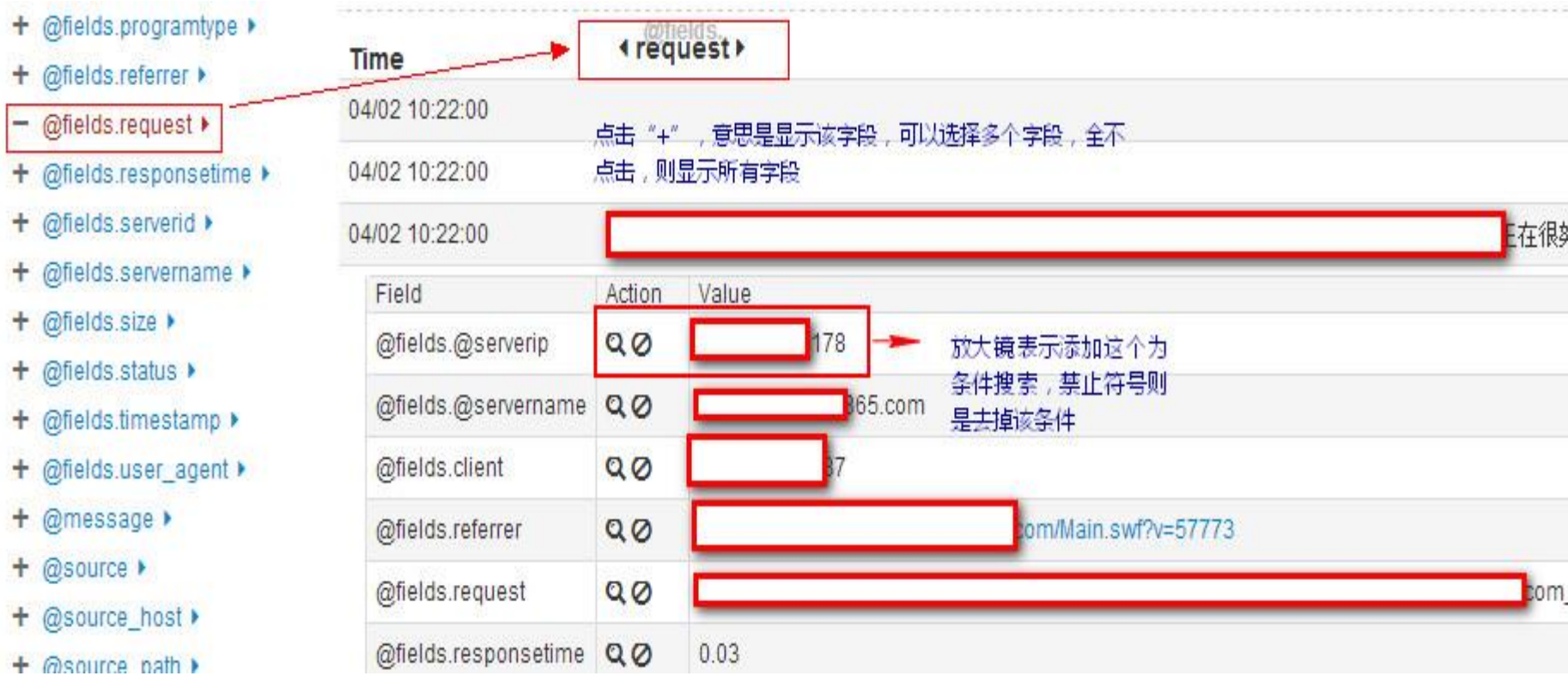
```
output
{
    #stdout { debug => true debug_format => "json" }
    elasticsearch
    {
        host => "127.0.0.1"
    }

    xmpp
    {
        tags => ['error_alert']
        host => "talk.google.com"
        message => "%{@source_host}: %{@message}"
        password => "xxxxxxxx"
        user => "xxxx@gmail.com"
        users => ["johncanlam@gmail.com"]
    }
}
```

GROK正则

- PHPLOG \[%{DATA:timestamp}\] (?:%{GREEDYDATA:php_error})
- 在线调试地址：http://grokdebug.herokuapp.com/


网络
grokdebug.herokuapp.com
Grok Debugger
Debugger
Discover
[20-May-2013 15:07:01] PHP Parse error: syntax error, unexpected '^' in
\[%{DATA:timestamp}\] (?:%{GREEDYDATA:php_error})
Keep Empty Captures
Named Captures Only
Singles
{
"timestamp": [
[
"20-May-2013 15:07:01"
]
],
"php_error": [
[
"PHP Parse error: syntax error, unexpected '^' in"
]
]
}

Kibana使用


+ @fields.programtype
+ @fields.referrer
− @fields.request
+ @fields.responsetime
+ @fields.serverid
+ @fields.servername
+ @fields.size
+ @fields.status
+ @fields.timestamp
+ @fields.user_agent
+ @message
+ @source
+ @source_host
+ @source_path
Time
@fields.request
04/02 10:22:00
04/02 10:22:00
04/02 10:22:00
点击“+”，意思是显示该字段，可以选择多个字段，全不点击，则显示所有字段
Field
Action
Value
@fields.@serverip
@fields.@servername
@fields.client
@fields.referrer
@fields.request
@fields.responsetime
0.03
放大镜表示添加这个为条件搜索，禁止符号则是去掉该条件

存在问题

- Beaver实时收集并发送日志
  - 无用日志
  - 日志量大会造成拥堵
- 日志是否传输成功无法得知
- 会丢日志

Q&A