利用ELK收集、分析、展现MYSQL相关日志

——任志强

背景

1、现状

日志特点：

▲ 海量数据

▲ 分散分布

▲ 分析、汇总

背景

2、日志系统

一个完整日志系统的特点：

▲ 收集 - 能够采集多种来源的日志数据

▲ 传输 - 能够稳定的把日志数据传输到中央系统

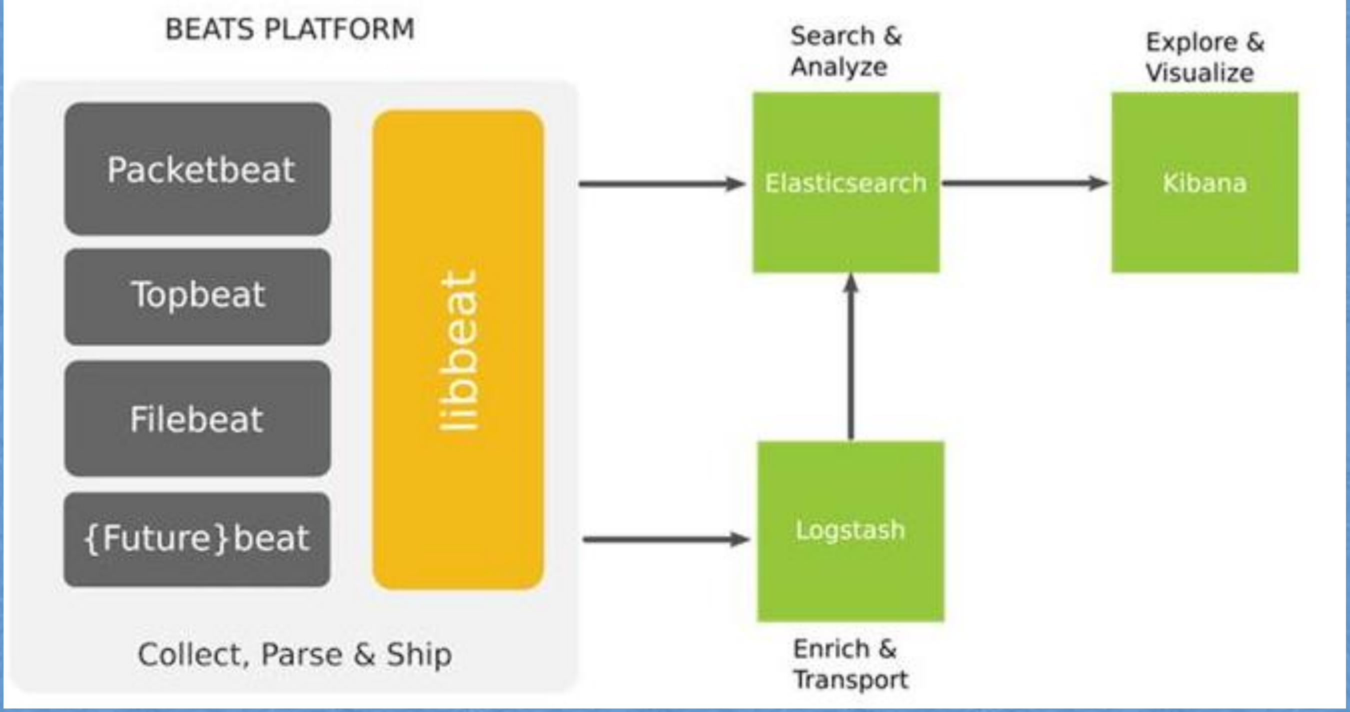
▲ 存储 - 如何存储日志数据

▲ 分析 - 可以支持 UI 分析

▲ 警告 - 能够提供错误报告，监控机制

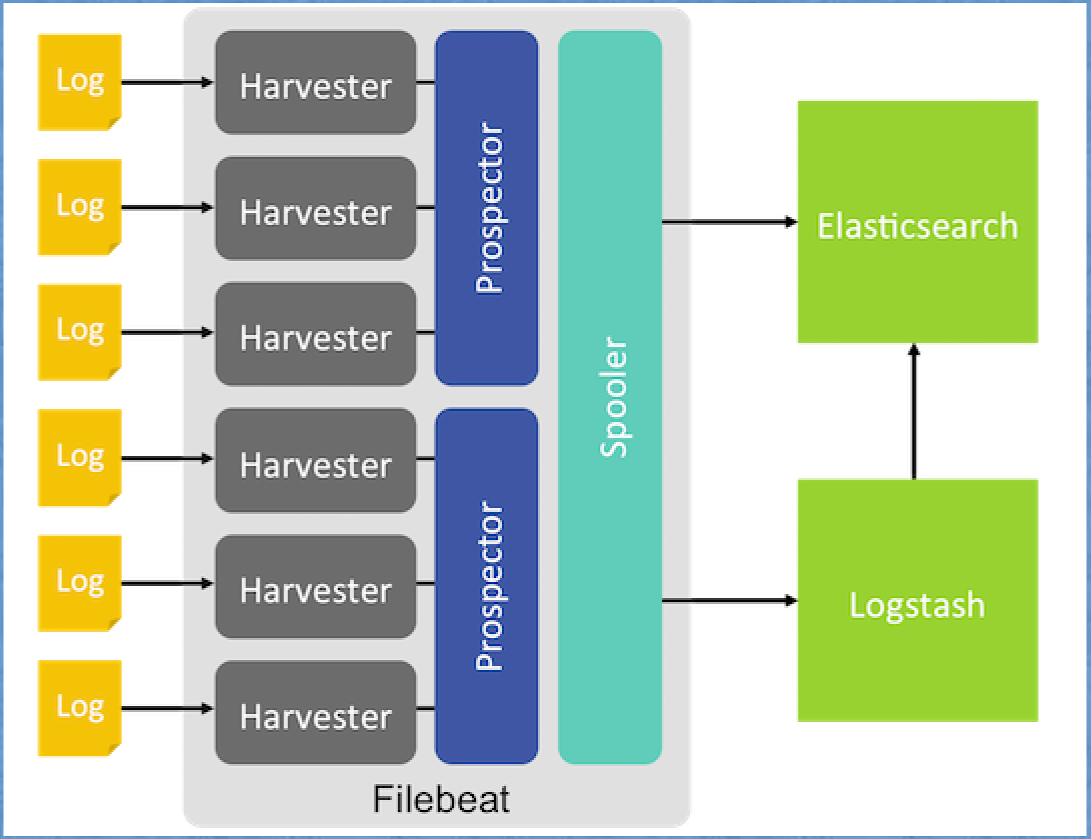
ELK介绍

1、架构


BEATS PLATFORM
Packetbeat
Topbeat
Filebeat
{Future}beat
libbeat
Collect, Parse & Ship
Search &
Analyze
Elasticsearch
Explore &
Visualize
Kibana
Logstash
Enrich &
Transport

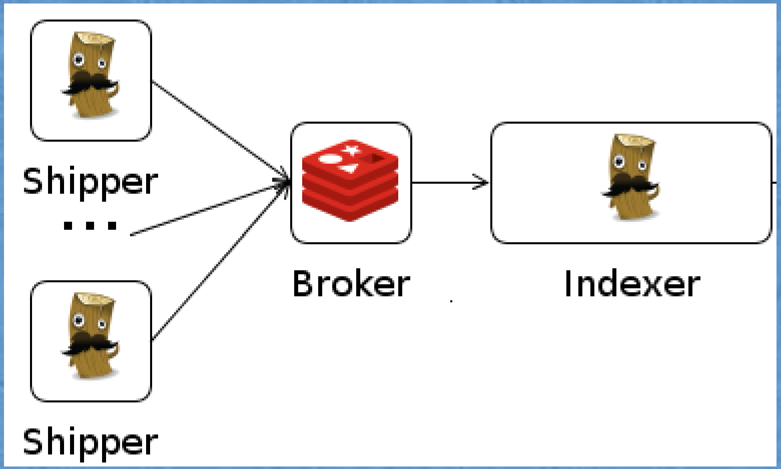
ELK介绍

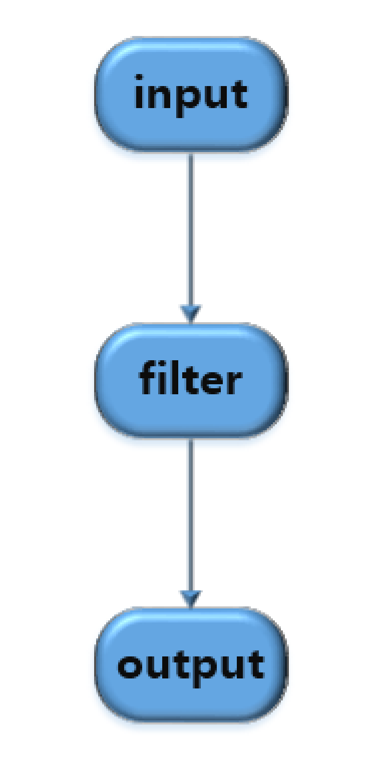
2、filebeat



ELK介绍

3、logstash





ELK介绍

3、logstash

插件：

logstash-input-file
logstash-input-redis
logstash-input-beats
…………
…………
logstash-filter-grok
logstash-filter-date
…………
…………
logstash-output-file
logstash-output-mongodb
logstash-output-elasticsearch
…………
…………

ELK介绍

4、elasticsearch

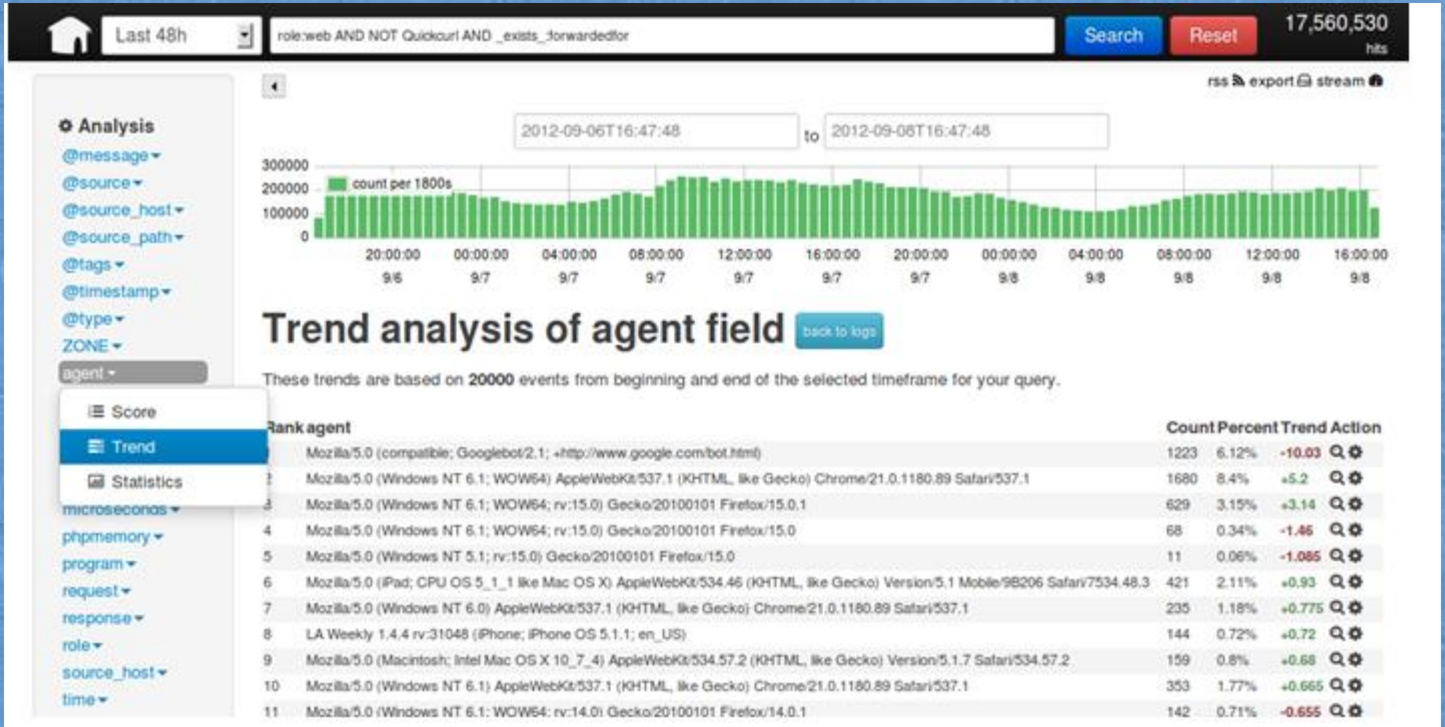
ElasticSearch是一个基于Lucene的搜索服务器。它不但包括了全文搜索功能，还可以进行以下工作:

- 分布式实时文件存储，并将每一个字段都编入索引，使其可以被搜索。
- 实时分析的分布式搜索引擎。
- 可以扩展到上百台服务器，处理PB级别的结构化或非结构化数据。

ELK介绍

5、kibana

Kibana 是一个为 Logstash 和 ElasticSearch 提供的日志分析的 Web 接口。可使用它对日志进行高效的搜索、可视化、分析等各种操作。



role:web AND NOT Quickcurl AND _exists_:forwardedfor

2012-09-06T16:47:48 to 2012-09-08T16:47:48

Trend analysis of agent field

These trends are based on **20000** events from beginning and end of the selected timeframe for your query.

Rank	agent	Count	Percent	Trend	Action
	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	1223	6.12%	-10.03	🔍 ⚙
2	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1	1680	8.4%	+5.2	🔍 ⚙
3	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:15.0) Gecko/20100101 Firefox/15.0.1	629	3.15%	+3.14	🔍 ⚙
4	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:15.0) Gecko/20100101 Firefox/15.0	68	0.34%	-1.46	🔍 ⚙
5	Mozilla/5.0 (Windows NT 5.1; rv:15.0) Gecko/20100101 Firefox/15.0	11	0.06%	-1.085	🔍 ⚙
6	Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3	421	2.11%	+0.93	🔍 ⚙
7	Mozilla/5.0 (Windows NT 6.0) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1	235	1.18%	+0.775	🔍 ⚙
8	LA Weekly 1.4.4 rv:31048 (iPhone; iPhone OS 5.1.1; en_US)	144	0.72%	+0.72	🔍 ⚙
9	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/534.57.2 (KHTML, like Gecko) Version/5.1.7 Safari/534.57.2	159	0.8%	+0.68	🔍 ⚙
10	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1	353	1.77%	+0.665	🔍 ⚙
11	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101 Firefox/14.0.1	142	0.71%	-0.655	🔍 ⚙

ELK安装配置

1、 安装

软件

序号	软件	版本
1	oracle jdk	jdk1.7.0_80
2	filebeat	filebeat-1.2.3
3	logstash	logstash-2.3.4
4	elasticsearch	elasticsearch-2.3.4
5	kibana	kibana-4.5.3

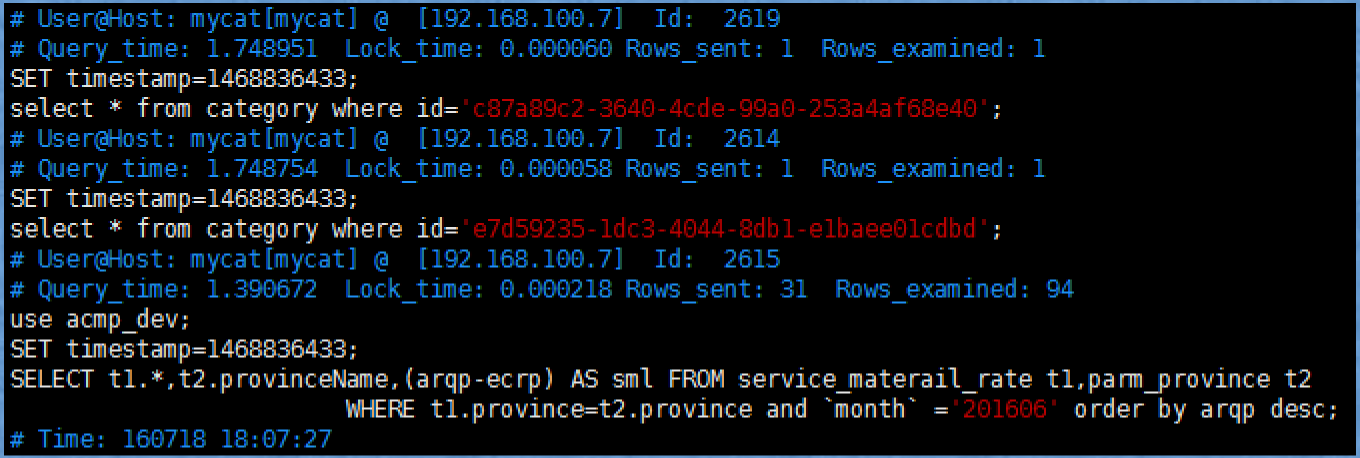
安装

解压至相关目录即可使用。

ELK安装配置

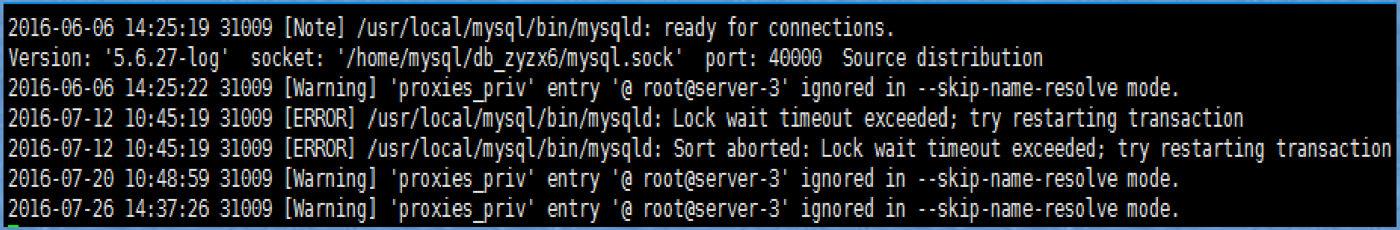
2、mysql相应日志格式

mysql slow log



```
# User@Host: mycat[mycat] @  [192.168.100.7]  Id:  2619
# Query_time: 1.748951  Lock_time: 0.000060 Rows_sent: 1  Rows_examined: 1
SET timestamp=1468836433;
select * from category where id='c87a89c2-3640-4cde-99a0-253a4af68e40';
# User@Host: mycat[mycat] @  [192.168.100.7]  Id:  2614
# Query_time: 1.748754  Lock_time: 0.000058 Rows_sent: 1  Rows_examined: 1
SET timestamp=1468836433;
select * from category where id='e7d59235-1dc3-4044-8db1-e1baee01cdbd';
# User@Host: mycat[mycat] @  [192.168.100.7]  Id:  2615
# Query_time: 1.390672  Lock_time: 0.000218 Rows_sent: 31  Rows_examined: 94
use acmp_dev;
SET timestamp=1468836433;
SELECT t1.*,t2.provinceName,(arqp-ecrp) AS sml FROM service_materail_rate t1,parm_province t2
                        WHERE t1.province=t2.province and `month` ='201606' order by arqp desc;
# Time: 160718 18:07:27
```

mysql error log



```
2016-06-06 14:25:19 31009 [Note] /usr/local/mysql/bin/mysqld: ready for connections.
Version: '5.6.27-log'  socket: '/home/mysql/db_zyzx6/mysql.sock'  port: 40000  Source distribution
2016-06-06 14:25:22 31009 [Warning] 'proxies_priv' entry '@ root@server-3' ignored in --skip-name-resolve mode.
2016-07-12 10:45:19 31009 [ERROR] /usr/local/mysql/bin/mysqld: Lock wait timeout exceeded; try restarting transaction
2016-07-12 10:45:19 31009 [ERROR] /usr/local/mysql/bin/mysqld: Sort aborted: Lock wait timeout exceeded; try restarting transaction
2016-07-20 10:48:59 31009 [Warning] 'proxies_priv' entry '@ root@server-3' ignored in --skip-name-resolve mode.
2016-07-26 14:37:26 31009 [Warning] 'proxies_priv' entry '@ root@server-3' ignored in --skip-name-resolve mode.
```

ELK安装配置

3、filebeat配置

slow log

```
filebeat:
  prospectors:
    -
      paths:
        - /home/mysql/renzq/slow.log
      encoding: utf-8
      fields:
        server_ip: xxx.xxx.xxx.xxx
        server_port: 40000
      fields_under_root: true
      multiline:
        pattern: "^# User@Host:"
        negate: true
        match: after
output:
  logstash:
    hosts: ["xxx.xxx.xxx.xxx:5044"]
logging:
  to_files: true
  files:
    path: ./logs
    name: filebeat
    rotateeverybytes: 10485760
    keepfiles: 7
```

ELK安装配置

3、filebeat配置

error log

```
filebeat:
  prospectors:
    -
       paths:
          - /home/mysql/renzq/mysql.err
       encoding: utf-8
       fields:
          server_ip: xxx.xxx.xxx.xxx
          server_port: 40000
       fields_under_root: true
       multiline:
          pattern: "^[[:digit:]]{4}-[[:digit:]]{2}-[[:digit:]]{2}"
          negate: true
          match: after
output:
  logstash:
    hosts: ["xxx.xxx.xxx.xxx:5044"]
logging:
  to_files: true
  files:
    path: ./logs
    name: filebeat
    rotateeverybytes: 10485760
    keepfiles: 7
```

ELK安装配置

4、logstash配置

DATE插件：

filters/date 插件可以用来转换你的日志记录中的时间字符串，变成 LogStash::Timestamp 对象，然后转存到 @timestamp 字段里。

outputs/elasticsearch 中常用的 %{+YYYY.MM.dd} 这种写法必须读取 @timestamp 数据

ELK安装配置

4、logstash配置

Grok插件：

1、已定义可以直接引用的

%{USERNAME:user}：[a-zA-Z0-9._-]+

%{DATA}： .*?

%{WORD}: \b\w+\b

2、自定义

(?<request_time>\d+(?:\.\d+)?)

3、判断

(?:\.\d+)?

ELK安装配置

4、logstash配置

slow log

```
# User@Host: mycat[mycat] @  [xxx.xxx.xxx.xxx]  Id:   161
# Query_time: 5.373068  Lock_time: 0.000042 Rows_sent: 0  Rows_examined: 1
use ngmmgw_dev;
SET timestamp=1471859932;
DELETE FROM ofPresence WHERE username='10086';
# Time: 160823 15:02:04
```

```
input {
  beats {
    port => 5044
    host => "xxx.xxx.xxx.xxx"
 }
}
filter {
  grok {
    match => { "message" => "(?m)^#
User@Host:\s+%{USER:user}\[%{USER}\]\s+@\s+\[%{IP:client_ip}\]\s+Id:\s+%{NUMBER:thread_id}\n#\s+Query_time:\s+%{NUMBER:
query_time:float}\s+Lock_time:\s+%{N
UMBER:lock_time:float}\s+Rows_sent:\s+%{NUMBER:rows_sent:int}\s+Rows_examined:\s+%{NUMBER:rows_examined:int}\n\s*(?:use
%{DATA:database};\s*\n)?SET timestamp=%{NUMBER:timestamp};\n\s*(?<sql>(?<action>\w+)\b.*;)\s*(?:\n# Time)?.*$"}        }
date {
    match => [ "timestamp", "UNIX" ,"yyyy-MM-dd HH:mm:ss"]
    remove_field => [ "timestamp" ]
  }
}
output {
  elasticsearch {
      hosts => ["xxx.xxx.xxx.xxx:9200"]
      index=>"slow-log-%{+YYYY.MM.dd}"
      flush_size => 2000
      idle_flush_time => 10
  }
  }
}
```

ELK安装配置

4、logstash配置

error log

```
2016-07-19 23:09:48 9941 [Note] Event Scheduler: Loaded 0 events
2016-07-19 23:09:48 9941 [Note] /usr/local/mysql/bin/mysqld: ready for connections.
Version: '5.6.27-log'  socket: '/home/mysql/db_zyzx5/mysql.sock'  port: 40000  Source distribution
2016-07-20 10:47:26 9941 [Warning] 'proxies_priv' entry '@ root@server-2' ignored in --skip-name-resolve mode.
```

```
input {
  beats {
    port => 5044
    host => "xxx.xxx.xxx.xxx"
 }
}

filter {
  grok {
    match => { "message" => "(?<timestamp>\d{4}-\d{2}-
\d{2}\s+\d{2}:\d{2}:\d{2})\s+%{NUMBER:pid:int}\s+\[%{DATA:level}\]\s+(?<content>.*)"}
  }
}
output {
  elasticsearch {
    hosts=>["xxx.xxx.xxx.xxx:9200"]
    index=>"error-log-%{+YYYY.MM.dd}"
    flush_size => 2000
    idle_flush_time => 10
        }
}
```

ELK安装配置

5、elasticsearch配置

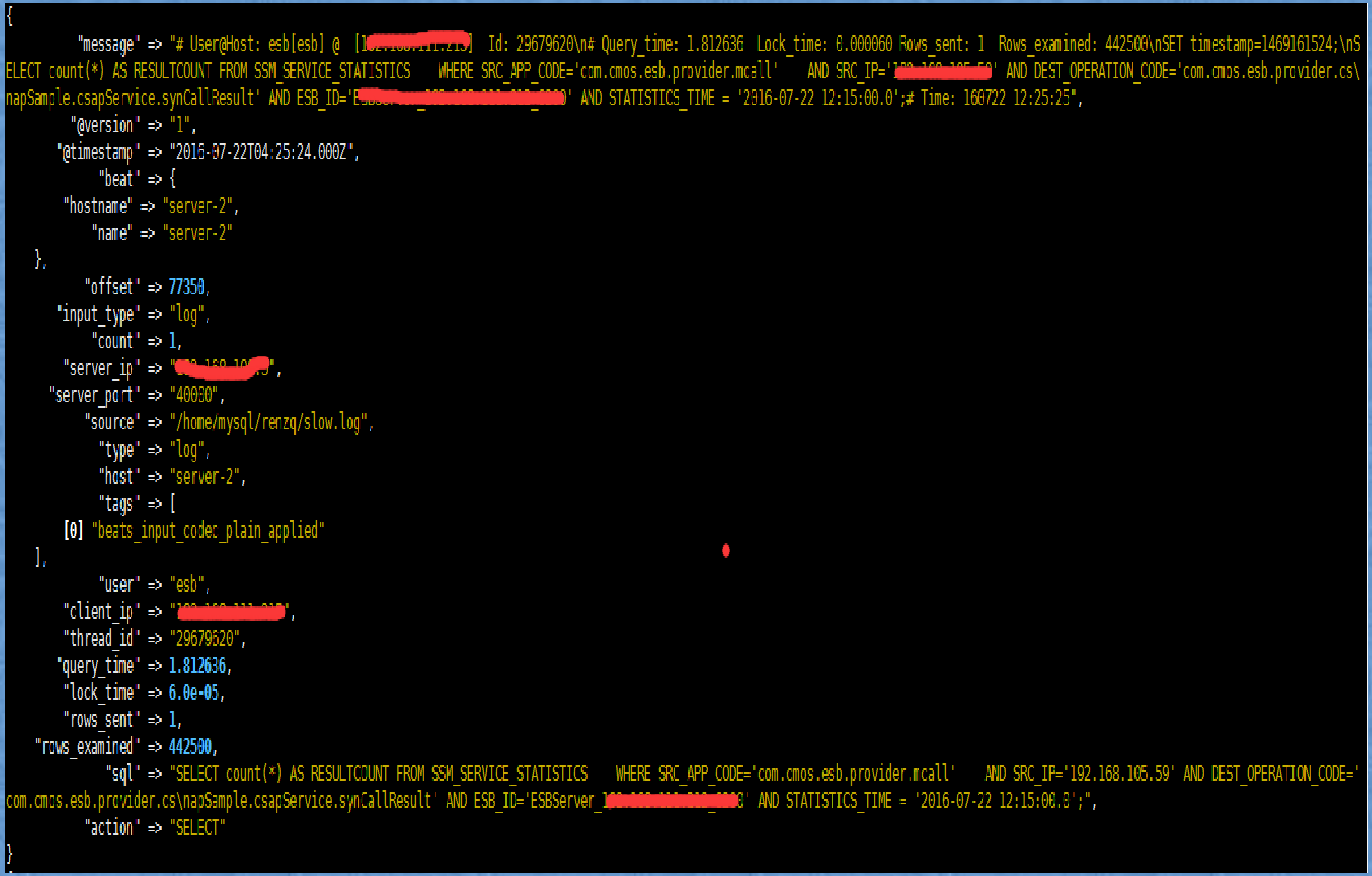
elasticsearch

```
cluster.name: carl
node.name: node-1
path.data: /home/mysql/renzq/data
path.logs: /home/mysql/renzq/log
network.host: xxx.xxx.xxx.xxx
http.port: 9200
```

ELK安装配置

5、elasticsearch配置

slow log

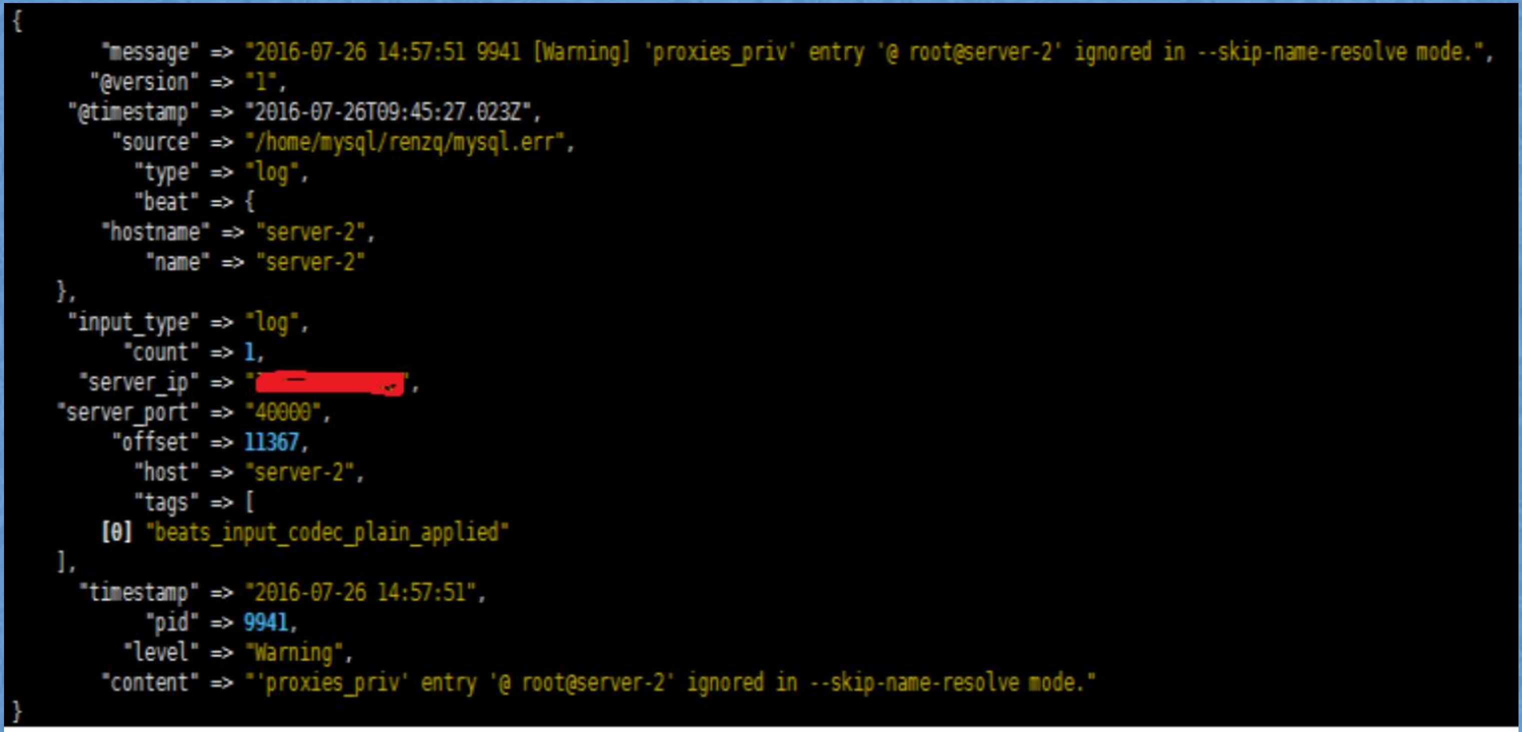


```
{
          "message" => "# User@Host: esb[esb] @  [[redacted]]  Id: 29679620\n# Query_time: 1.812636  Lock_time: 0.000060 Rows_sent: 1  Rows_examined: 442500\nSET timestamp=1469161524;\nSELECT count(*) AS RESULTCOUNT FROM SSM_SERVICE_STATISTICS    WHERE SRC_APP_CODE='com.cmos.esb.provider.mcall'    AND SRC_IP='[redacted]' AND DEST_OPERATION_CODE='com.cmos.esb.provider.cs\napSample.csapService.synCallResult' AND ESB_ID='[redacted]' AND STATISTICS_TIME = '2016-07-22 12:15:00.0';# Time: 160722 12:25:25",
         "@version" => "1",
       "@timestamp" => "2016-07-22T04:25:24.000Z",
             "beat" => {
        "hostname" => "server-2",
            "name" => "server-2"
    },
           "offset" => 77350,
       "input_type" => "log",
            "count" => 1,
        "server_ip" => "[redacted]",
      "server_port" => "40000",
           "source" => "/home/mysql/renzq/slow.log",
             "type" => "log",
             "host" => "server-2",
             "tags" => [
        [0] "beats_input_codec_plain_applied"
    ],
             "user" => "esb",
        "client_ip" => "[redacted]",
        "thread_id" => "29679620",
       "query_time" => 1.812636,
        "lock_time" => 6.0e-05,
        "rows_sent" => 1,
    "rows_examined" => 442500,
              "sql" => "SELECT count(*) AS RESULTCOUNT FROM SSM_SERVICE_STATISTICS    WHERE SRC_APP_CODE='com.cmos.esb.provider.mcall'    AND SRC_IP='192.168.105.59' AND DEST_OPERATION_CODE='com.cmos.esb.provider.cs\napSample.csapService.synCallResult' AND ESB_ID='ESBServer_[redacted]' AND STATISTICS_TIME = '2016-07-22 12:15:00.0';",
           "action" => "SELECT"
}
```

ELK安装配置

5、elasticsearch配置

error log



```
{
        "message" => "2016-07-26 14:57:51 9941 [Warning] 'proxies_priv' entry '@ root@server-2' ignored in --skip-name-resolve mode.",
       "@version" => "1",
     "@timestamp" => "2016-07-26T09:45:27.023Z",
         "source" => "/home/mysql/renzq/mysql.err",
           "type" => "log",
           "beat" => {
        "hostname" => "server-2",
            "name" => "server-2"
    },
     "input_type" => "log",
          "count" => 1,
      "server_ip" => "[redacted]",
    "server_port" => "40000",
         "offset" => 11367,
           "host" => "server-2",
           "tags" => [
        [0] "beats_input_codec_plain_applied"
    ],
      "timestamp" => "2016-07-26 14:57:51",
            "pid" => 9941,
          "level" => "Warning",
        "content" => "'proxies_priv' entry '@ root@server-2' ignored in --skip-name-resolve mode."
}
```

ELK安装配置

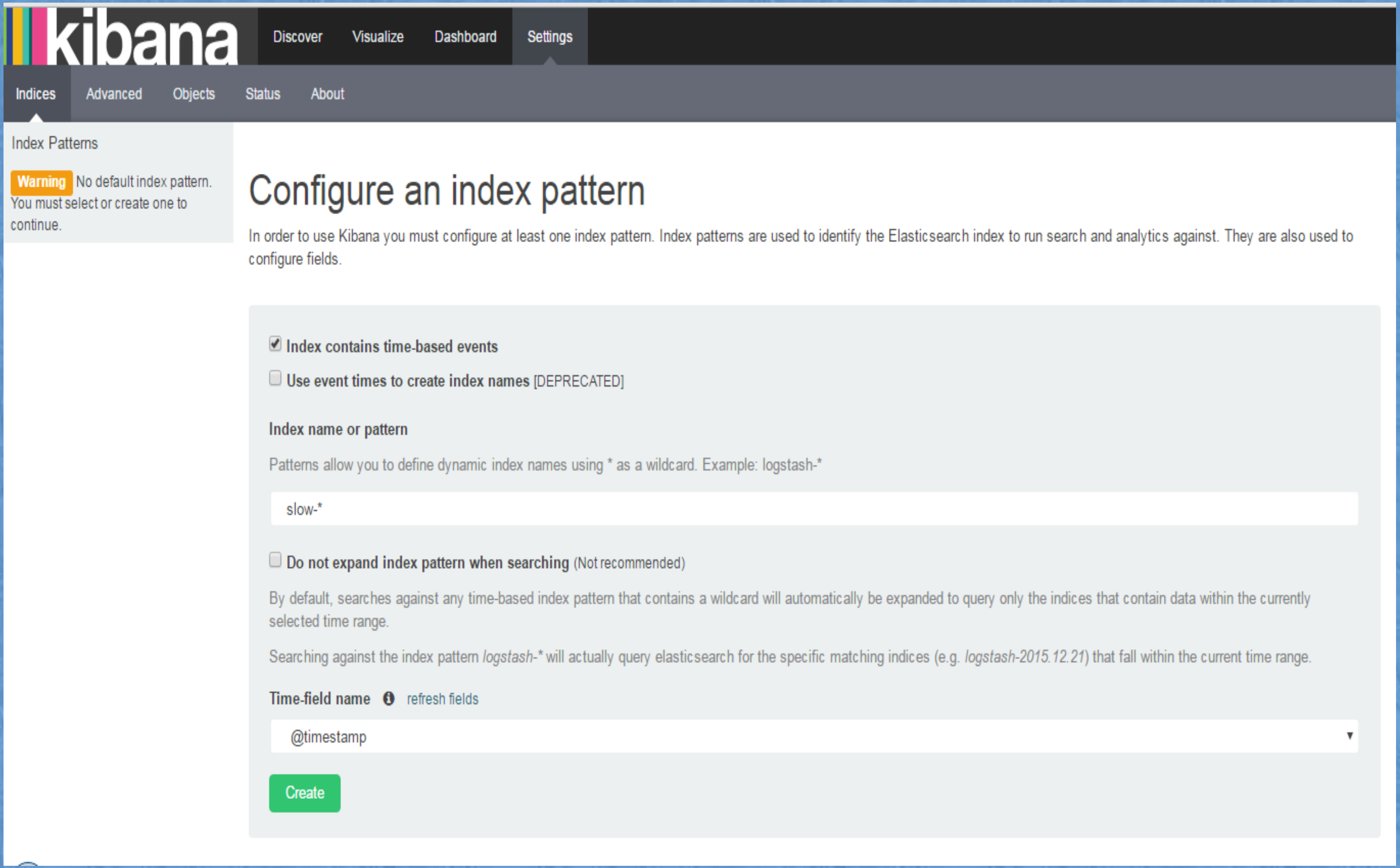
5、kibana配置

kibana

```
server.port: 5601
server.host: "0.0.0.0"
elasticsearch.url: "http://xxx.xxx.xxx.xxx:9200"
```

ELK安装配置

5、kibana配置



Warning No default index pattern. You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☑ **Index contains time-based events**

☐ **Use event times to create index names** [DEPRECATED]

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

slow-*

☐ **Do not expand index pattern when searching** (Not recommended)

By default, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-** will actually query elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

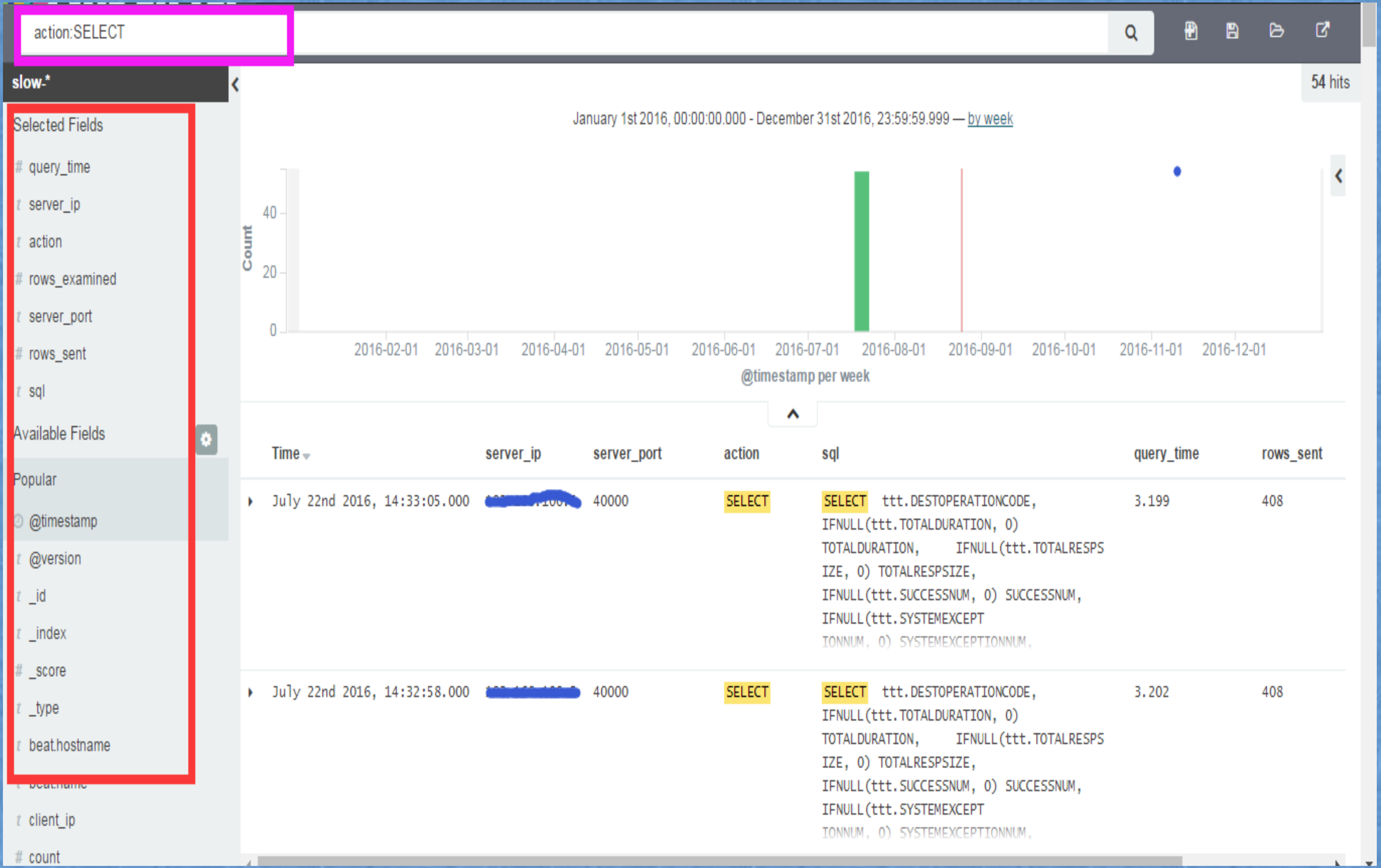
Time-field name ℹ refresh fields

@timestamp ▾

Create

日志展现

1、 slow log



action:SELECT

slow-*

54 hits

Selected Fields

- query_time
- server_ip
- action
- rows_examined
- server_port
- rows_sent
- sql

Available Fields

Popular

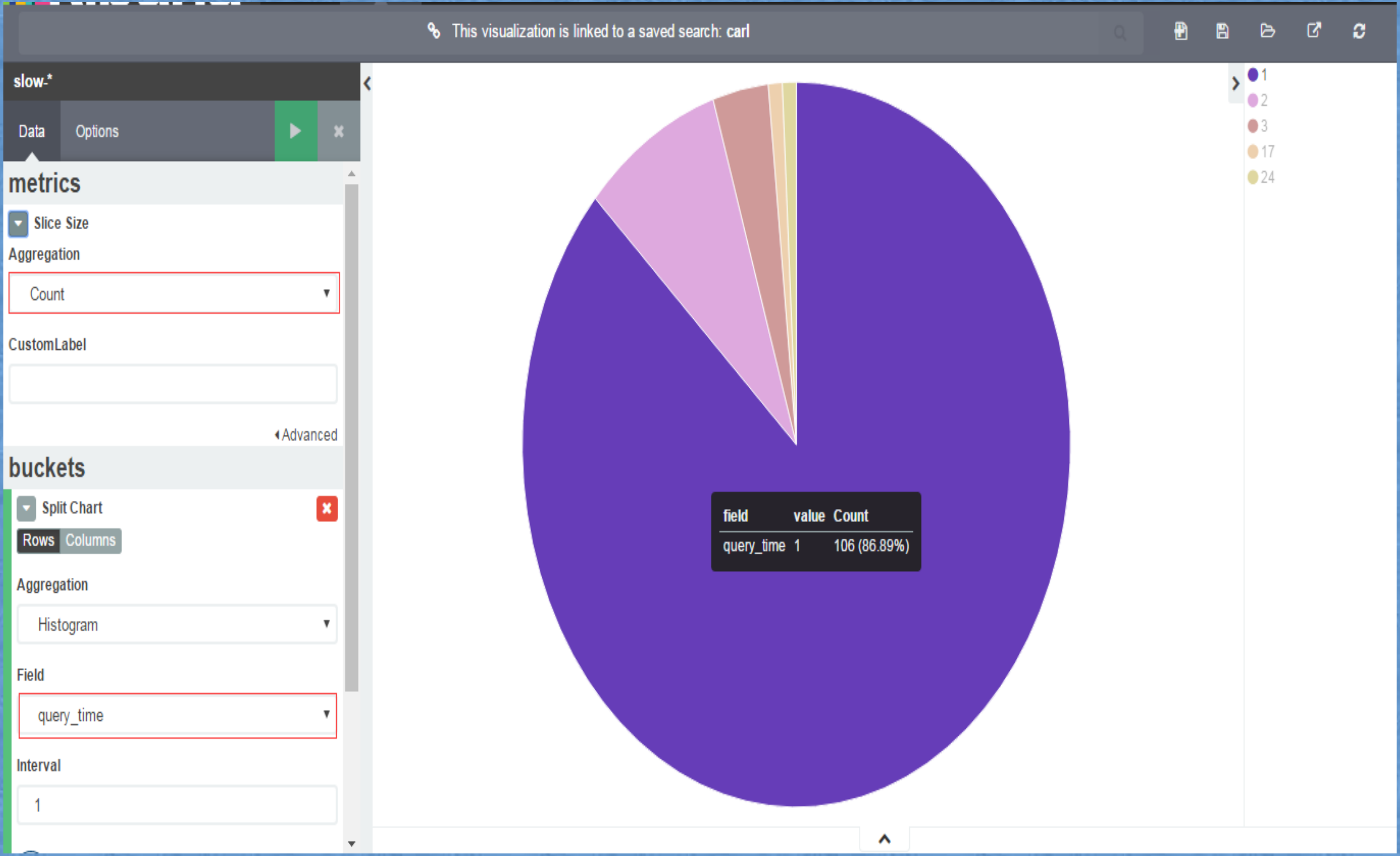
- @timestamp
- @version
- _id
- _index
- _score
- _type
- beat.hostname
- beat.name
- client_ip
- count

January 1st 2016, 00:00:00.000 - December 31st 2016, 23:59:59.999 — by week

Time	server_ip	server_port	action	sql	query_time	rows_sent
July 22nd 2016, 14:33:05.000	[redacted]	40000	SELECT	SELECT ttt.DESTOPERATIONCODE, IFNULL(ttt.TOTALDURATION, 0) TOTALDURATION, IFNULL(ttt.TOTALRESPSIZE, 0) TOTALRESPSIZE, IFNULL(ttt.SUCCESSNUM, 0) SUCCESSNUM, IFNULL(ttt.SYSTEMEXCEPTIONNUM, 0) SYSTEMEXCEPTIONNUM,	3.199	408
July 22nd 2016, 14:32:58.000	[redacted]	40000	SELECT	SELECT ttt.DESTOPERATIONCODE, IFNULL(ttt.TOTALDURATION, 0) TOTALDURATION, IFNULL(ttt.TOTALRESPSIZE, 0) TOTALRESPSIZE, IFNULL(ttt.SUCCESSNUM, 0) SUCCESSNUM, IFNULL(ttt.SYSTEMEXCEPTIONNUM, 0) SYSTEMEXCEPTIONNUM,	3.202	408

日志展现

1、 slow log



This visualization is linked to a saved search: carl

slow-*

metrics

Slice Size

Aggregation: Count

CustomLabel

buckets

Split Chart

Aggregation: Histogram

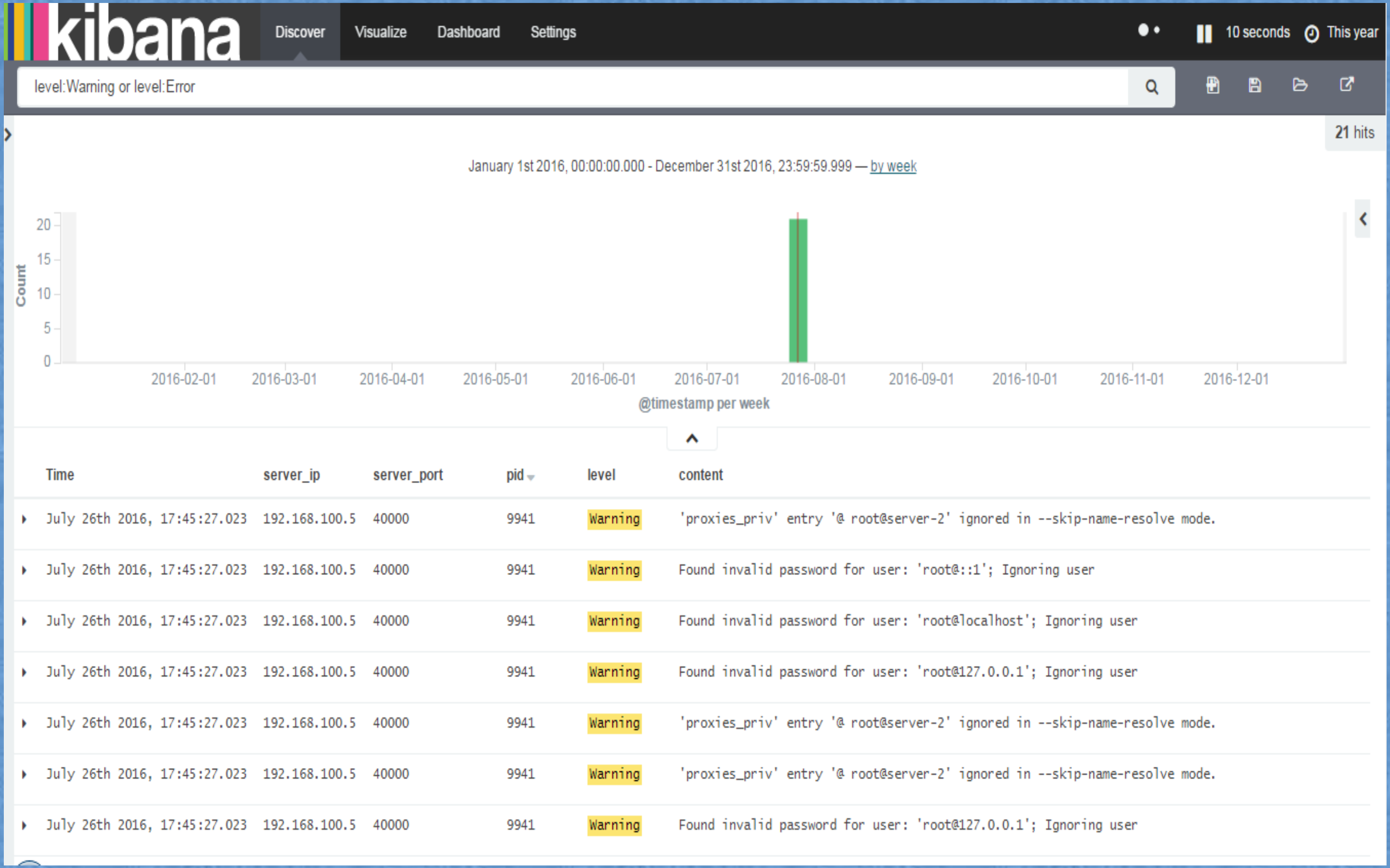
Field: query_time

Interval: 1

field	value	Count
query_time	1	106 (86.89%)

日志展现

1、error log



level:Warning or level:Error

January 1st 2016, 00:00:00.000 - December 31st 2016, 23:59:59.999 — by week

Time	server_ip	server_port	pid	level	content
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	'proxies_priv' entry '@ root@server-2' ignored in --skip-name-resolve mode.
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	Found invalid password for user: 'root@::1'; Ignoring user
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	Found invalid password for user: 'root@localhost'; Ignoring user
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	Found invalid password for user: 'root@127.0.0.1'; Ignoring user
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	'proxies_priv' entry '@ root@server-2' ignored in --skip-name-resolve mode.
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	'proxies_priv' entry '@ root@server-2' ignored in --skip-name-resolve mode.
July 26th 2016, 17:45:27.023	192.168.100.5	40000	9941	Warning	Found invalid password for user: 'root@127.0.0.1'; Ignoring user