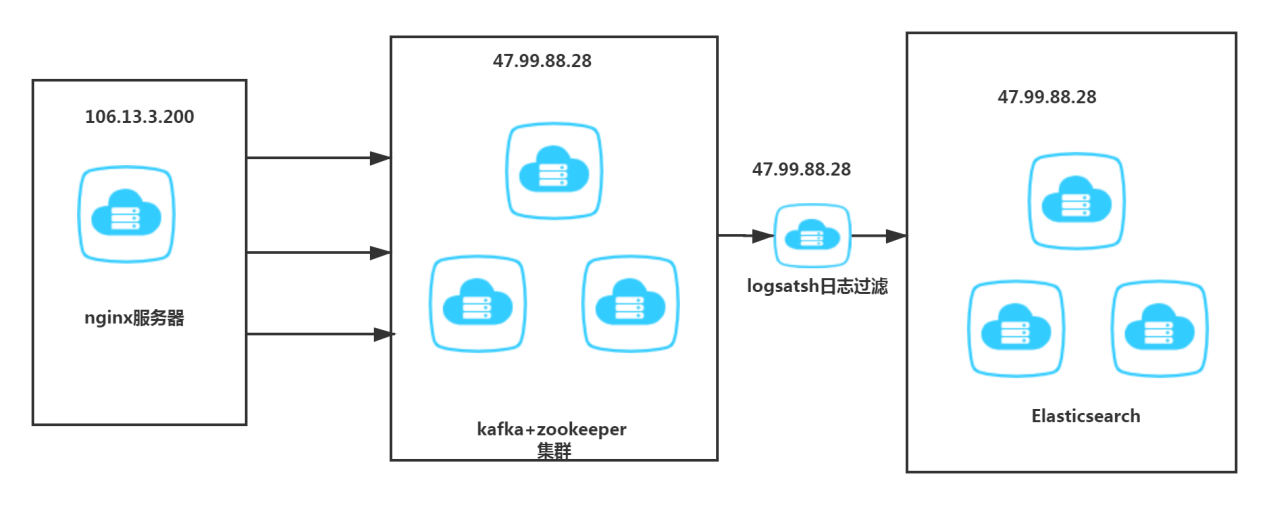
Elk收集mysql 慢日志及性能的优化

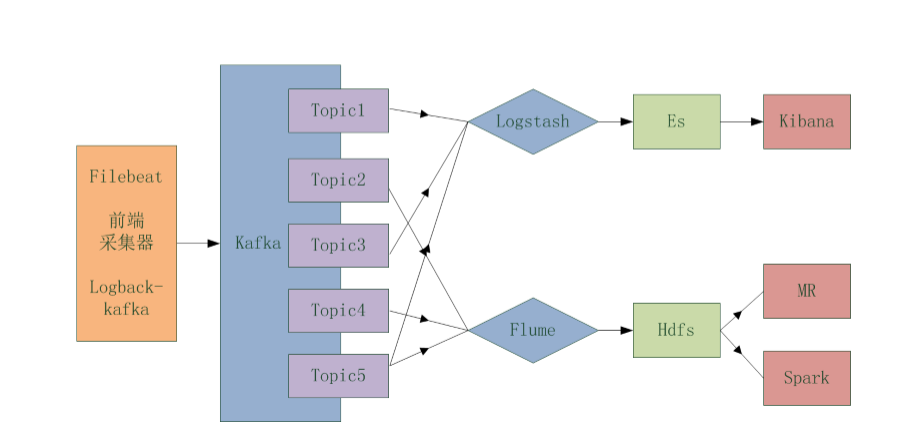
# 1前言

本篇以ELK+Filebeat+Kafka+ZooKeeper构建慢查询日志分析平台的架构进行文档撰写，完整的拓扑结构如下图所示：



软件 | 版本 | 备注 |  
| --- | --- |--- |-  
| centos| 7.5 | |  
| JDK | 1.8 |on 47.99.88.28 |  
| zookeeper| 3.4.8 | on 47.99.88.28|  
| kafka| 2.12-2.1.0 | on 47.99.88.28 |  
| elasticsearch| 6.5.4 |on 47.99.88.28 |  
| ZooInspector| |on windows |  
| filebeat| 6.5.4|on 106.13.3.200 |  
| logstash|6.5.4 |on 47.99.88.28 |

# 2 系统拓扑



**kafka**是一种高吞吐量的分布式发布订阅消息系统，它可以处理消费者规模的网站中的所有动作流数据。

**ZooKeeper**是一个分布式的，开放源码的分布式应用程序协调服务，是Google的Chubby一个开源的实现，是Hadoop和Hbase的重要组件。它是一个为分布式应用

提供一致性服务的软件，提供的功能包括：配置维护、域名服务、分布式同步、组服务等。

# 3服务器

|  |  |  |
| --- | --- | --- |
| **软件** | **版本** | **备注** |
| Mysql | 5.7 |  |
| Jdk | 1.8 |  |
| Filebeat | 6.5.4 |  |
| Logstash | 6.5.4 |  |

# 4 启动各服务

1. 启动zookeeper ：./bin/zkServer.sh start
2. 启动kafka：./bin/kafka-server-start.sh -daemon config/server.properties
3. 查看java进程pid

jps -l

4512 org.apache.zookeeper.server.quorum.QuorumPeerMain  
10069 kafka.Kafka

Create a topic

./bin/kafka-topics.sh --create --zookeeper localhost:2181 --replication-factor 1 --partitions 1 --topic test

查看 topic

./bin/kafka-topics.sh --list --zookeeper localhost:2181

##查询 topic 详细信息

./bin/kafka-topics.sh --describe --zookeeper localhost:2181 --topic test

1. 启动mysql

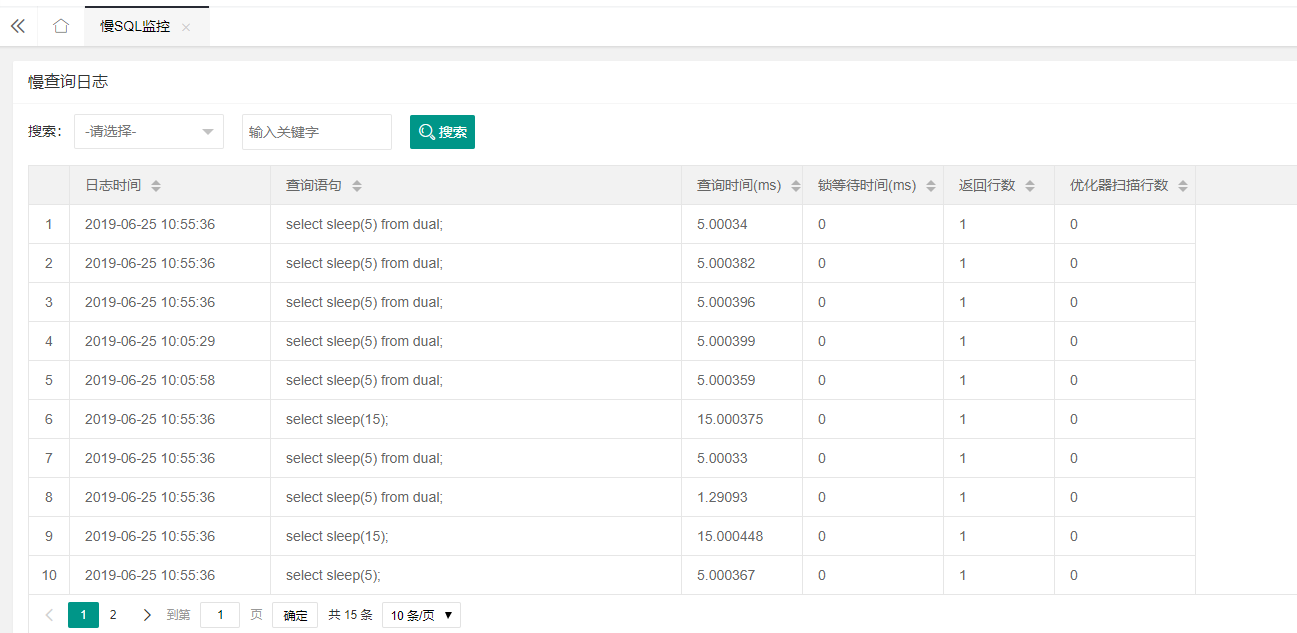
systemctl start mysqld

开发远程登录权限：

GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY '1q2w3e4r' WITH GRANT OPTION;  
FLUSH PRIVILEGES;

# 5 mysql 慢日志查询

在应用程序连接mysql过程中，某些sql语句由于写的不是很标准，会导致执行完毕所花费的时间特别长，SQL语句执行时间过长，势必影响业务系统的使用，这个时候可能就会出现开发人员和运维人员相互扯皮的问题，其实通过ELK工具，就可以轻松解决：开启mysql慢查询日志，然后将日志收集到统一展示平台，每个SQL语句的写法、执行时间、读取时间等等指标可以通过前端展现。



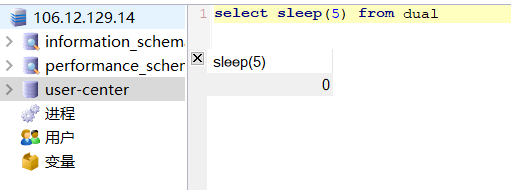
## 5.1 开启mysql慢查询日志

mysql> show variables like "%log\_output%";  
mysql> show variables like "%slow%";  
mysql> show variables like "%long\_query\_time%";  
mysql> set global slow\_query\_log=ON;  
mysql> set global long\_query\_time=1 ;  
mysql> select @@global.long\_query\_time from dual

为了让设置永久生效，可将上面配置写入my.cnf文件中，编辑/etc/my.cnf，添加如下内容：  
#是否开启慢查询日志  
slow\_query\_log=ON  
#日志存放地址  
slow\_query\_log\_file=/db/data/sql-slow.log  
#慢查询时间(s)  
long\_query\_time=1

重启mysql

## 5.2 登录执行慢查询



cat /db/data/sql-slow.log

# Time: 2020-08-08T01:54:40.924740Z

# User@Host: root[root] @ [118.212.184.230] Id: 3283

# Query\_time: 5.000408 Lock\_time: 0.000000 Rows\_sent: 1 Rows\_examined: 0

SET timestamp=1561427680;

select sleep(5) from dual;

# 6 FileBeat

1. 下载

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-6.5.4-linux-x86\_64.tar.gz

tar -zxvf filebeat-6.5.4-linux-x86\_64.tar.gz -C /usr/local/

cd /usr/local/filebeat-6.5.4-linux-x86\_64

1. 配置

Vi filebeat.yml

filebeat.inputs:

- type: log

enable: true

paths:

- /db/data/sql-slow.log

fields:

log\_topic: mysqlslowlogs

exclude\_lines: ['^\# Time']

multiline:

pattern: '^\# Time|^\# User'

negate: true

match: after

processors:

- drop\_fields:

fields: ["beat" ,"input" , "source" ,"offset" ,"prospector"]

filebeat.config.modules:

path: ${path.config}/modules.d/\*.yml

reload.enabled: false

output.kafka:

enabled: true

hosts: ["47.99.88.28:9092"]

topic: '%{[fields.log\_topic]}'

partition.round\_robin:

reachable\_only: true

required\_acks: 1

compression: gzip

max\_message\_bytes: 1000000

logging.level: debug

启动：nohup ./filebeat -e -c filebeat.yml >&/dev/null &

# 7 logstatsh

## 7.1 下载

wget https://artifacts.elastic.co/downloads/logstash/logstash-6.5.4.tar.gz

tar -zxvf logstash-6.5.4.tar.gz -C /usr/local/

cd logstash-6.5.4/

ls

cd bin

## 7.2 配置

input {

kafka {

enable\_auto\_commit => true

auto\_commit\_interval\_ms => "1000"

bootstrap\_servers => "47.99.88.28:9092"

topics => ["mysqlslowlogs"]

}

}

filter {

json {

source => "message"

}

grok {

match => [ "message", "^#\s+User@Host:\s+%{USER:user}\[[^\]]+\]\s+@\s+(?:(?<clienthost>\S\*) )?\[(?:%{IP:clientip})?\]\s+Id:\s+%{NUMBER:id}\n# Query\_time: %{NUMBER:query\_time}\s+Lock\_time: %{NUMBER:lock\_time}\s+Rows\_sent: %{NUMBER:rows\_sent}\s+Rows\_examined: %{NUMBER:rows\_examined}\nuse\s(?<dbname>\w+);\nSET\s+timestamp=%{NUMBER:timestamp\_mysql};\n(?<query>[\s\S]\*)" ]

match => [ "message", "^#\s+User@Host:\s+%{USER:user}\[[^\]]+\]\s+@\s+(?:(?<clienthost>\S\*) )?\[(?:%{IP:clientip})?\]\s+Id:\s+%{NUMBER:id}\n# Query\_time: %{NUMBER:query\_time}\s+Lock\_time: %{NUMBER:lock\_time}\s+Rows\_sent: %{NUMBER:rows\_sent}\s+Rows\_examined: %{NUMBER:rows\_examined}\nSET\s+timestamp=%{NUMBER:timestamp\_mysql};\n(?<query>[\s\S]\*)" ]

match => [ "message", "^#\s+User@Host:\s+%{USER:user}\[[^\]]+\]\s+@\s+(?:(?<clienthost>\S\*) )?\[(?:%{IP:clientip})?\]\n# Query\_time: %{NUMBER:query\_time}\s+Lock\_time: %{NUMBER:lock\_time}\s+Rows\_sent: %{NUMBER:rows\_sent}\s+Rows\_examined: %{NUMBER:rows\_examined}\nuse\s(?<dbname>\w+);\nSET\s+timestamp=%{NUMBER:timestamp\_mysql};\n(?<query>[\s\S]\*)" ]

match => [ "message", "^#\s+User@Host:\s+%{USER:user}\[[^\]]+\]\s+@\s+(?:(?<clienthost>\S\*) )?\[(?:%{IP:clientip})?\]\n# Query\_time: %{NUMBER:query\_time}\s+Lock\_time: %{NUMBER:lock\_time}\s+Rows\_sent: %{NUMBER:rows\_sent}\s+Rows\_examined: %{NUMBER:rows\_examined}\nSET\s+timestamp=%{NUMBER:timestamp\_mysql};\n(?<query>[\s\S]\*)" ]

}

date {

match => ["timestamp\_mysql","yyyy-MM-dd HH:mm:ss.SSS","UNIX"]

}

date {

match => ["timestamp\_mysql","yyyy-MM-dd HH:mm:ss.SSS","UNIX"]

target => "timestamp"

}

mutate {

convert => ["query\_time", "float"]

convert => ["lock\_time", "float"]

convert => ["rows\_sent", "integer"]

convert => ["rows\_examined", "integer"]

remove\_field => "message"

remove\_field => "timestamp\_mysql"

remove\_field => "@version"

}

}

output {

elasticsearch {

hosts => ["47.99.88.28:9200"]

index => "mysql-slowlog-%{+YYYY.MM.dd}"

}

stdout{

codec=> rubydebug

}

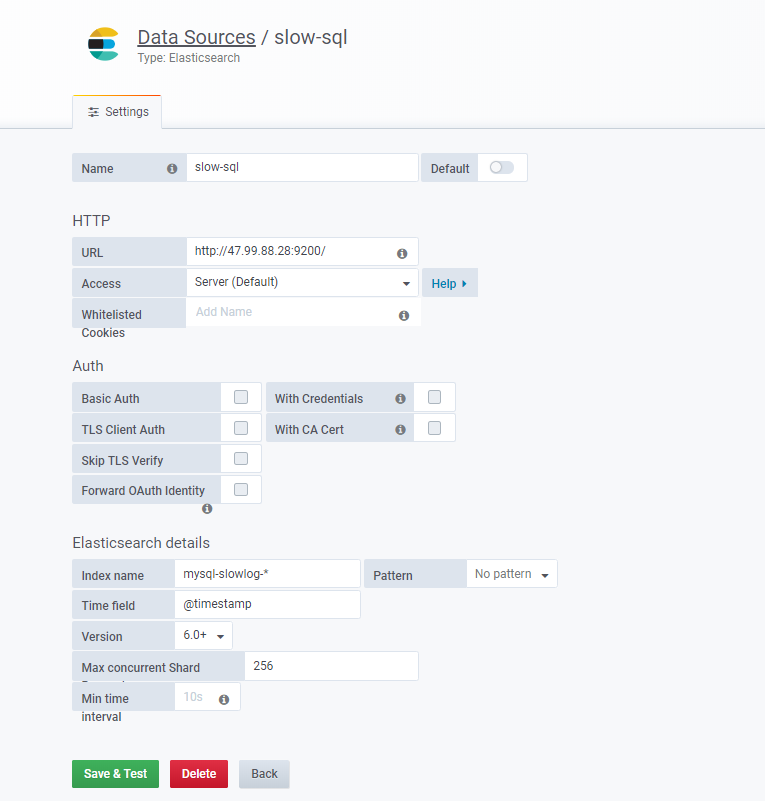
}

## 7.3 启动

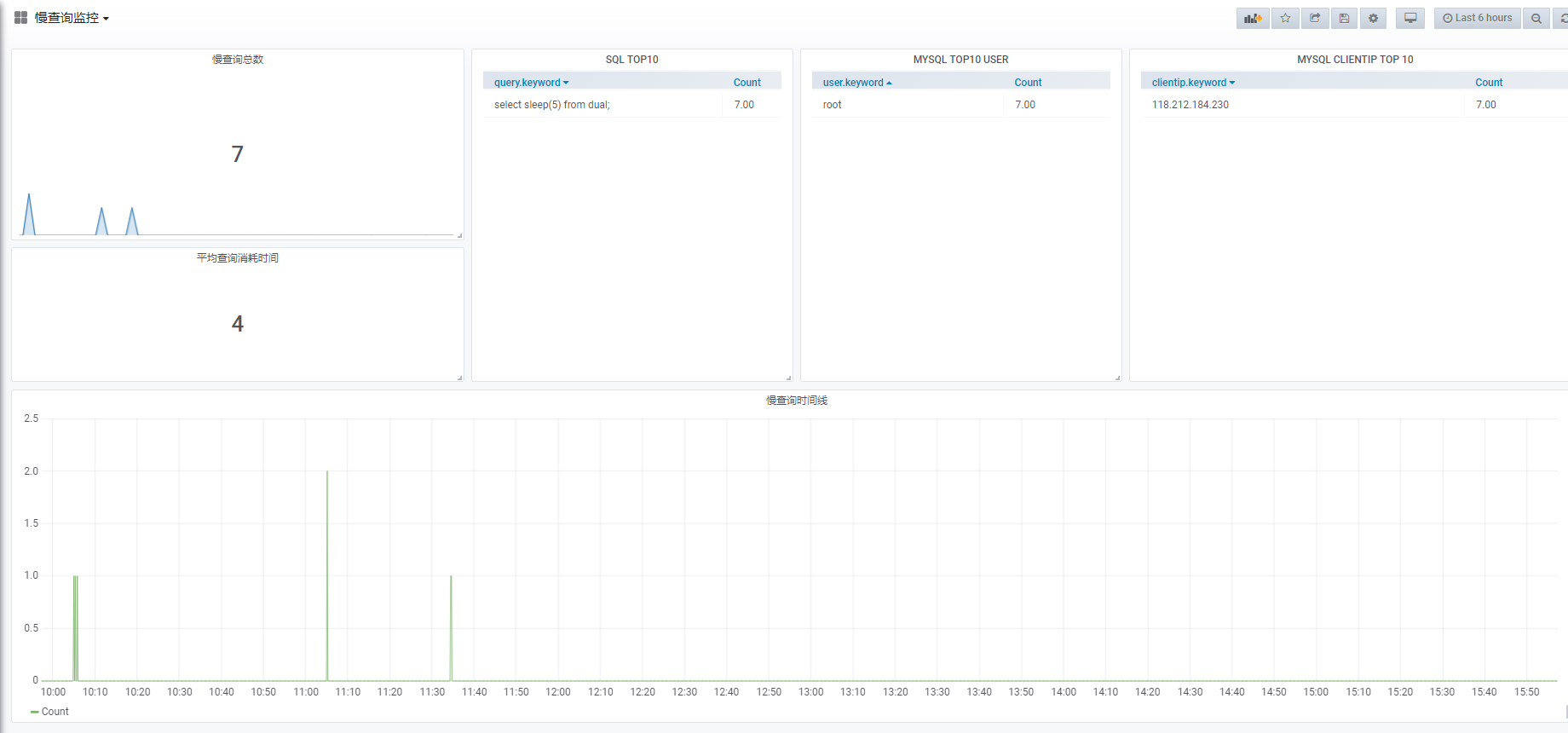
nohup ./logstash -f logstash.conf >&/dev/null &

# 8 grafana

## 8.1 配置数据源



导入



{

"annotations": {

"list": [

{

"builtIn": 1,

"datasource": "-- Grafana --",

"enable": true,

"hide": true,

"iconColor": "rgba(0, 211, 255, 1)",

"name": "Annotations & Alerts",

"type": "dashboard"

}

]

},

"editable": true,

"gnetId": null,

"graphTooltip": 0,

"id": 13,

"links": [],

"panels": [

{

"cacheTimeout": null,

"colorBackground": false,

"colorValue": false,

"colors": [

"#299c46",

"rgba(237, 129, 40, 0.89)",

"#d44a3a"

],

"datasource": "slow-sql",

"format": "short",

"gauge": {

"maxValue": 100,

"minValue": 0,

"show": false,

"thresholdLabels": false,

"thresholdMarkers": true

},

"gridPos": {

"h": 7,

"w": 7,

"x": 0,

"y": 0

},

"id": 2,

"interval": null,

"links": [],

"mappingType": 1,

"mappingTypes": [

{

"name": "value to text",

"value": 1

},

{

"name": "range to text",

"value": 2

}

],

"maxDataPoints": 100,

"nullPointMode": "connected",

"nullText": null,

"postfix": "",

"postfixFontSize": "50%",

"prefix": "",

"prefixFontSize": "50%",

"rangeMaps": [

{

"from": "null",

"text": "N/A",

"to": "null"

}

],

"sparkline": {

"fillColor": "rgba(31, 118, 189, 0.18)",

"full": false,

"lineColor": "rgb(31, 120, 193)",

"show": true

},

"tableColumn": "",

"targets": [

{

"bucketAggs": [

{

"field": "@timestamp",

"id": "2",

"settings": {

"interval": "auto",

"min\_doc\_count": 0,

"trimEdges": 0

},

"type": "date\_histogram"

}

],

"metrics": [

{

"field": "select field",

"id": "1",

"type": "count"

}

],

"refId": "A",

"timeField": "@timestamp"

}

],

"thresholds": "",

"timeFrom": null,

"timeShift": null,

"title": "慢查询总数",

"type": "singlestat",

"valueFontSize": "80%",

"valueMaps": [

{

"op": "=",

"text": "N/A",

"value": "null"

}

],

"valueName": "total"

},

{

"columns": [],

"datasource": "slow-sql",

"fontSize": "100%",

"gridPos": {

"h": 12,

"w": 5,

"x": 7,

"y": 0

},

"id": 6,

"links": [],

"pageSize": null,

"scroll": true,

"showHeader": true,

"sort": {

"col": 0,

"desc": true

},

"styles": [

{

"alias": "Time",

"dateFormat": "YYYY-MM-DD HH:mm:ss",

"pattern": "Time",

"type": "date"

},

{

"alias": "",

"colorMode": null,

"colors": [

"rgba(245, 54, 54, 0.9)",

"rgba(237, 129, 40, 0.89)",

"rgba(50, 172, 45, 0.97)"

],

"decimals": 2,

"pattern": "/.\*/",

"thresholds": [],

"type": "number",

"unit": "short"

}

],

"targets": [

{

"bucketAggs": [

{

"field": "query.keyword",

"id": "2",

"settings": {

"min\_doc\_count": 1,

"order": "desc",

"orderBy": "\_term",

"size": "10"

},

"type": "terms"

}

],

"metrics": [

{

"field": "select field",

"id": "1",

"type": "count"

}

],

"query": "\*",

"refId": "A",

"timeField": "@timestamp"

}

],

"timeFrom": null,

"timeShift": null,

"title": "SQL TOP10",

"transform": "table",

"type": "table"

},

{

"columns": [],

"datasource": "slow-sql",

"fontSize": "100%",

"gridPos": {

"h": 12,

"w": 5,

"x": 12,

"y": 0

},

"id": 10,

"links": [],

"pageSize": null,

"scroll": true,

"showHeader": true,

"sort": {

"col": 0,

"desc": false

},

"styles": [

{

"alias": "Time",

"dateFormat": "YYYY-MM-DD HH:mm:ss",

"pattern": "Time",

"type": "date"

},

{

"alias": "",

"colorMode": null,

"colors": [

"rgba(245, 54, 54, 0.9)",

"rgba(237, 129, 40, 0.89)",

"rgba(50, 172, 45, 0.97)"

],

"decimals": 2,

"pattern": "/.\*/",

"thresholds": [],

"type": "number",

"unit": "short"

}

],

"targets": [

{

"bucketAggs": [

{

"field": "user.keyword",

"id": "2",

"settings": {

"min\_doc\_count": 1,

"order": "desc",

"orderBy": "\_term",

"size": "10"

},

"type": "terms"

}

],

"metrics": [

{

"field": "select field",

"id": "1",

"type": "count"

}

],

"query": "\*",

"refId": "A",

"timeField": "@timestamp"

}

],

"timeFrom": null,

"timeShift": null,

"title": "MYSQL TOP10 USER",

"transform": "table",

"type": "table"

},

{

"columns": [],

"datasource": "slow-sql",

"fontSize": "100%",

"gridPos": {

"h": 12,

"w": 7,

"x": 17,

"y": 0

},

"id": 12,

"links": [],

"pageSize": null,

"scroll": true,

"showHeader": true,

"sort": {

"col": 0,

"desc": true

},

"styles": [

{

"alias": "Time",

"dateFormat": "YYYY-MM-DD HH:mm:ss",

"pattern": "Time",

"type": "date"

},

{

"alias": "",

"colorMode": null,

"colors": [

"rgba(245, 54, 54, 0.9)",

"rgba(237, 129, 40, 0.89)",

"rgba(50, 172, 45, 0.97)"

],

"decimals": 2,

"pattern": "/.\*/",

"thresholds": [],

"type": "number",

"unit": "short"

}

],

"targets": [

{

"bucketAggs": [

{

"field": "clientip.keyword",

"id": "2",

"settings": {

"min\_doc\_count": 1,

"order": "desc",

"orderBy": "\_term",

"size": "10"

},

"type": "terms"

}

],

"metrics": [

{

"field": "select field",

"id": "1",

"type": "count"

}

],

"refId": "A",

"timeField": "@timestamp"

}

],

"timeFrom": null,

"timeShift": null,

"title": "MYSQL CLIENTIP TOP 10",

"transform": "table",

"type": "table"

},

{

"cacheTimeout": null,

"colorBackground": false,

"colorValue": false,

"colors": [

"#299c46",

"rgba(237, 129, 40, 0.89)",

"#d44a3a"

],

"datasource": "slow-sql",

"format": "short",

"gauge": {

"maxValue": 100,

"minValue": 0,

"show": false,

"thresholdLabels": false,

"thresholdMarkers": true

},

"gridPos": {

"h": 5,

"w": 7,

"x": 0,

"y": 7

},

"id": 4,

"interval": null,

"links": [],

"mappingType": 1,

"mappingTypes": [

{

"name": "value to text",

"value": 1

},

{

"name": "range to text",

"value": 2

}

],

"maxDataPoints": 100,

"nullPointMode": "connected",

"nullText": null,

"postfix": "",

"postfixFontSize": "50%",

"prefix": "",

"prefixFontSize": "50%",

"rangeMaps": [

{

"from": "null",

"text": "N/A",

"to": "null"

}

],

"sparkline": {

"fillColor": "rgba(31, 118, 189, 0.18)",

"full": false,

"lineColor": "rgb(31, 120, 193)",

"show": false

},

"tableColumn": "",

"targets": [

{

"bucketAggs": [

{

"field": "@timestamp",

"id": "2",

"settings": {

"interval": "auto",

"min\_doc\_count": 0,

"trimEdges": 0

},

"type": "date\_histogram"

}

],

"metrics": [

{

"field": "query\_time",

"id": "1",

"meta": {},

"settings": {},

"type": "avg"

}

],

"refId": "A",

"timeField": "@timestamp"

}

],

"thresholds": "",

"timeFrom": null,

"timeShift": null,

"title": "平均查询消耗时间",

"type": "singlestat",

"valueFontSize": "80%",

"valueMaps": [

{

"op": "=",

"text": "N/A",

"value": "null"

}

],

"valueName": "avg"

},

{

"aliasColors": {},

"bars": false,

"dashLength": 10,

"dashes": false,

"datasource": "slow-sql",

"fill": 1,

"gridPos": {

"h": 12,

"w": 24,

"x": 0,

"y": 12

},

"id": 8,

"legend": {

"avg": false,

"current": false,

"max": false,

"min": false,

"show": true,

"total": false,

"values": false

},

"lines": true,

"linewidth": 1,

"links": [],

"nullPointMode": "null",

"percentage": false,

"pointradius": 2,

"points": false,

"renderer": "flot",

"seriesOverrides": [],

"spaceLength": 10,

"stack": false,

"steppedLine": false,

"targets": [

{

"bucketAggs": [

{

"field": "@timestamp",

"id": "2",

"settings": {

"interval": "auto",

"min\_doc\_count": 0,

"trimEdges": 0

},

"type": "date\_histogram"

}

],

"metrics": [

{

"field": "select field",

"id": "1",

"type": "count"

}

],

"refId": "A",

"timeField": "@timestamp"

}

],

"thresholds": [],

"timeFrom": null,

"timeRegions": [],

"timeShift": null,

"title": "慢查询时间线",

"tooltip": {

"shared": true,

"sort": 0,

"value\_type": "individual"

},

"type": "graph",

"xaxis": {

"buckets": null,

"mode": "time",

"name": null,

"show": true,

"values": []

},

"yaxes": [

{

"format": "short",

"label": null,

"logBase": 1,

"max": null,

"min": null,

"show": true

},

{

"format": "short",

"label": null,

"logBase": 1,

"max": null,

"min": null,

"show": true

}

],

"yaxis": {

"align": false,

"alignLevel": null

}

}

],

"schemaVersion": 18,

"style": "dark",

"tags": [],

"templating": {

"list": []

},

"time": {

"from": "now-6h",

"to": "now"

},

"timepicker": {

"refresh\_intervals": [

"5s",

"10s",

"30s",

"1m",

"5m",

"15m",

"30m",

"1h",

"2h",

"1d"

],

"time\_options": [

"5m",

"15m",

"1h",

"6h",

"12h",

"24h",

"2d",

"7d",

"30d"

]

},

"timezone": "",

"title": "慢查询监控",

"uid": "SSoUAD4Wz",

"version": 9

}

# 9 统一日志中心性能优化

## 9.1 fileBeat性能调优

filebeat在没有日志可采集情况下，的确不会占用太大的内存开销（一般在100M左右），但在有大量的日志需要采集时，filebeat的内存占用是没有固定值的，根据我们的使用经验，如果出现单条日志大于50KB，并且有瞬间爆发量的时候， filebeat的内存占用将会大于300MB，甚至，如果出现了极端情况，例如单条日志>10M时，即使filebeat会截断到10M，那么filebeat的内存占用也会达到20GB，这就很可怕了。filebeat作为日志采集agent，是需要部署到生产服务器上的，因此对filebeat的配置和调优至关重要，不合理的设置会导致filebeat占用过量的系统资源，造成内存泄露，还会影响生产服务器的正常运行。

要合理配置filebeat，就需要理解filebeat的工作机制以及运行原理，与logstash相比，filebeat虽然占用系统资源很少，但是在日志量比较大的情况下或者日志异常突发时，filebeat也会占用大量系统内存开销，因而，合理设置filebeat的配置参数十分重要。

### 9.1.1内存优化

Filebeat内存限制，有两种模式，一种是内存模式，一种是文件缓存模式，实际应用中任选其一即可。

内存模式：  
需要注意的是，所有事件（events）都是保存在内存中的，此模式只能限制事件数，无法限制最大使用内存，这有可能会因为日志长度导致内存使用暴增，相关配置如下：

queue.mem:

events: 4096 #表示队列可以存储的事件数量。默认值是4096个事件。

flush.min\_events: 512 #发布所需的最小事件数量。 默认值是0，表示可以直接输出发布事件，而无需额外的等待时间。 如果设置为非0，必须等待，在满足指定的事件数量后才能输出发布事件。

flush.timeout: 5s #表示最早的可用事件在队列中等待的最长时间，超过这个时间，立即输出发布事件，默认值是0s，表示立即可以输出发布事件

文件缓存模式：  
此模式可以限制最大使用内存，在filebeat6.3版本以后可以使用此功能，相关配置如下:

queue.spool:

file:

path: "${path.data}/spool.dat" #Spool file的路径

size: 512MiB #Spool file的大小，也就是缓冲区的大小。

page\_size: 16MiB #文件的页面大小。默认值为4096（4KiB）。

write:

buffer\_size: 10MiB #写缓冲区大小。一旦超过缓冲区大小，就刷新写缓冲区。

flush.timeout: 5s #写缓冲区中最旧事件的最长等待时间。如果设置为0，则在write.flush.events或write.buffer\_size满足时写入缓冲区仅刷新一次。

flush.events: 1024 #缓冲事件的数量。一旦达到上限，就刷新写缓冲区。

上面这个配置的含义如下：

Spool file将所有事件存储在磁盘的缓冲区中（内存中），如果已写入10MiB内容或1024个事件，则刷新写入缓冲区。如果最旧的可用事件在写缓冲区中等待5秒，则也将刷新写入缓冲区。

除了内存使用优化，filebeat还可以设置CPU最大使用核数，通过如下选项即可定义：

### 9.1.2文件系统资源优化

filebeat对日志的采集是贪婪的，只要发现日志就会坚持把日志采集完，否则会永久持有文件句柄不会“放手”，即使文件被删除。因此，filebeat在收集大量日志的时候，如果配置参数设置不当，会导致文件系统大量文件句柄被filebeat占用，导致收集日志异常，因此需要对filebeat采集日志的策略进行优化，常见的优化参数有如下几个：

close\_inactive: 1m  
表示没有新日志采集后多长时间关闭文件句柄，默认5分钟，设置成1分钟，加快文件句柄关闭；

close\_timeout: 3h  
表示传输了3h后在没有传输完成的话就强行关闭文件句柄，这个配置项是解决文件句柄耗尽的问题。但是开了这个配置项会有丢数据的风险。需要综合考虑。

clean\_inactive: 72h  
表示多久清理一次文件描述在registry文件，默认值是0表示不清理，不清理的意思是采集过的文件描述在registry文件里永不清理，在运行一段时间后，registry会变大，可能会带来性能问题。

ignore\_older: 70h  
上面设置了clean\_inactive，就需要设置ignore\_older，且要保证ignore\_older < clean\_inactive。

综述，filebeat调优其实就是调整参数的过程，max\_message\_bytes,queue.mem.events,queue.mem.flush.min\_events，以及队列占用内存的公式:max\_message\_bytes \* queue.mem.events

推荐采用内存模式，下面举例说明：

output.kafka:

enabled: true

# max\_message\_bytes: 1000000

hosts: ["10.60.x.x:9092"]

topic: '%{[fields][topic]}'

max\_procs: 4

#queue.mem.events: 4096

#queue.mem.flush.min\_events: 512

#queue.mem.flush.timeout: 5s

但其实，不同的环境下，不同的原因都可能会造成filebeat占用的内存过大，此时，需要仔细的确认你的上下文环境：是否因为通配符的原因，造成同时监控数量巨大的文件，这种情况应该避免用通配符监控无用的文件。是否文件的单行内容巨大，确定是否需要改造文件内容，或者将其过滤是否过多的匹配了multiline的pattern，并且多行的event是否单条体积过大。这时，就需要暂时关闭multiline，修改文件内容或者multiline的pattern。是否output经常阻塞，event queue里面总是一直缓存event。这时要检查你的网络环境或者消息队列等中间件是否正常