



GOPS2017
Beijing




GOPS

全球运维大会

2017



指导单位:  数据中心联盟
Data Center Alliance

主办单位:  高联运维社区
GreatOps Community

 开放运维联盟
OpenOps Alliance

大会时间: 7月26-30日

大会地点: 北京朝阳悠唐皇冠假日酒店



自动化运维之日志平台

赵班长 速云科技



GOPS2017
Beijing

目录

- ➔ **1** 基于开源的全链路自动化运维体系
- 2** Elastic Stack介绍
- 3** Elasticsearch入门
- 4** LogStash实战入门
- 5** 架构解耦之消息队列
- 6** Kibana简介和企业实践

讲师介绍



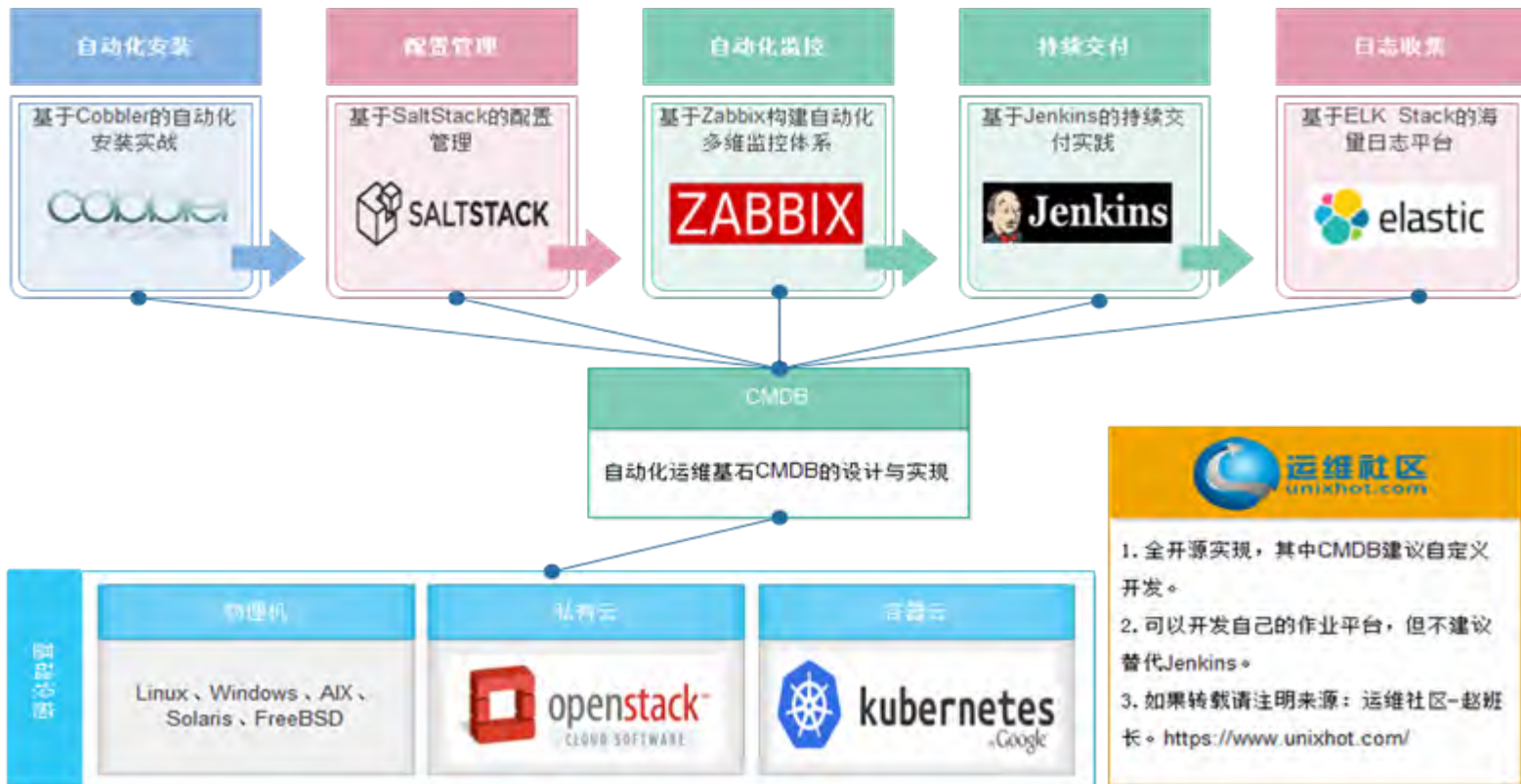
赵舜东

- 花名：“赵班长”，曾在武警某部负责指挥自动化的架构和运维工作，2008年退役后一直从事互联网运维工作，历任运维工程师、运维经理、运维架构师、运维总监。中国SaltStack用户组发起人、《SaltStack入门与实践》作者、《运维知识体系》作者、Exin DevOps Master认证讲师、GOPS金牌讲师。
 - ◆ 速云科技：<https://www.linuxhot.com/>
 - ◆ 运维社区：<https://www.unixhot.com/>



GOPS2017
Beijing

全链路自动化运维体系



运维社区
unixhot.com

1. 全开源实现，其中CMDB建议自定义开发。
2. 可以开发自己的作业平台，但不建议替代Jenkins。
3. 如果转载请注明来源：运维社区-赵班长。 <https://www.unixhot.com/>

基于Cobbler的自动化系统安装



```
Cobbler : http://cobbler.github.com

(local)
CentOS-7.1-x86_64

Press [Tab] to edit options

Automatic boot in 17 seconds...
```



GOPS2017
Beijing

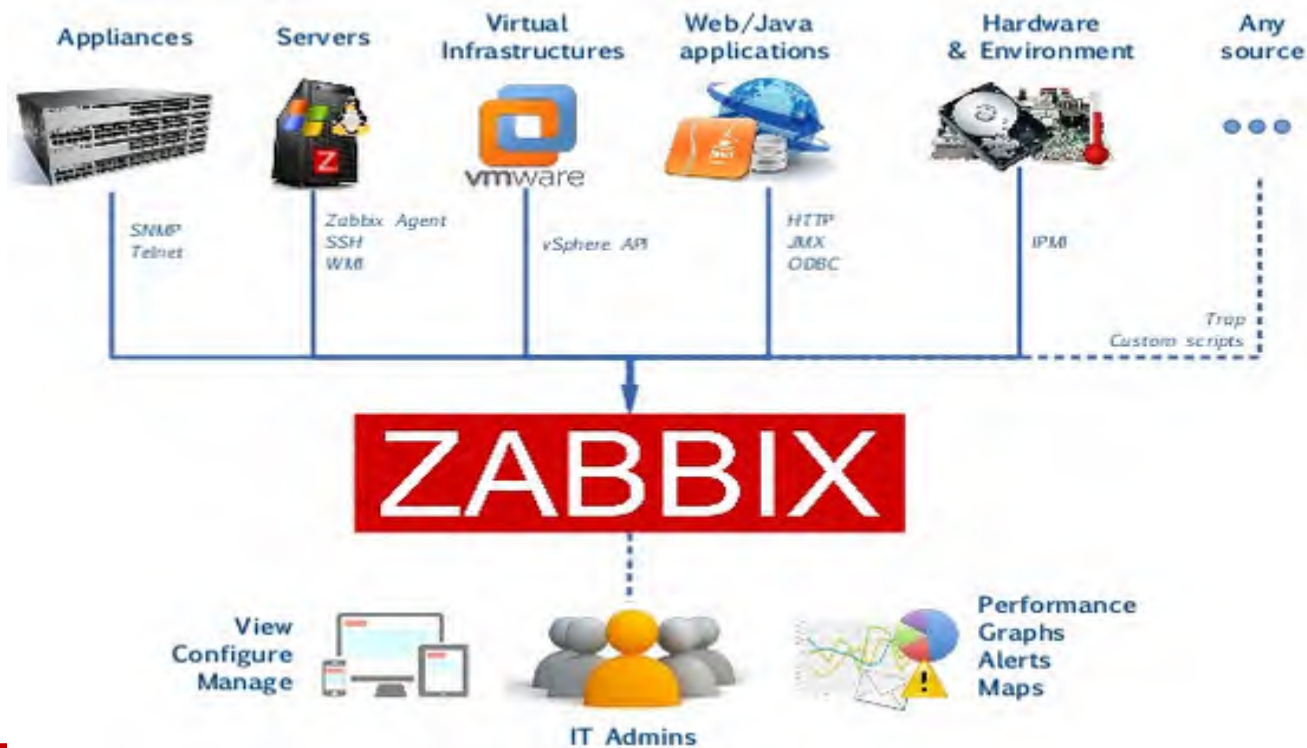
基于SaltStack的状态管理



基于Zabbix的自动化监控平台



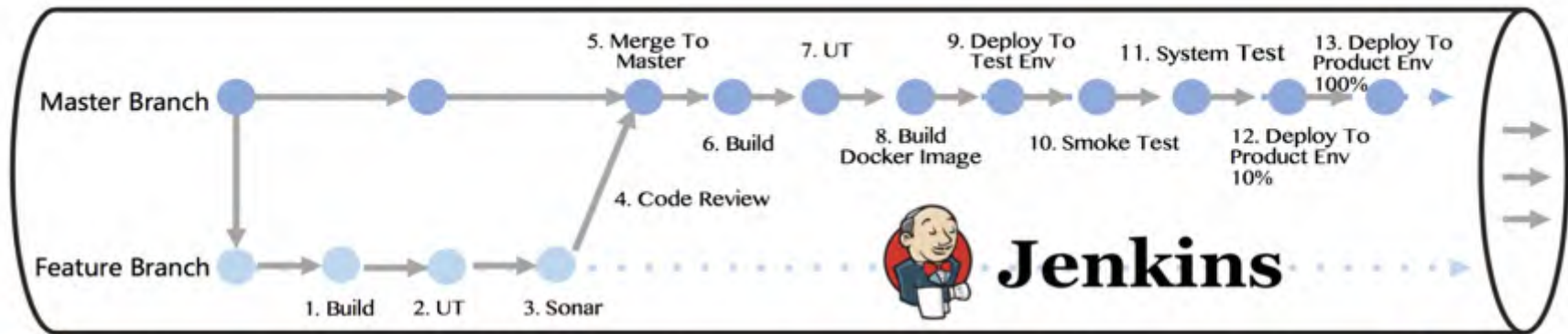
GOPS2017
Beijing



基于Jenkins的持续交付平台



GOPS2017
Beijing



Maven™

JUnit



GitLab

Nexus

sonarqube



HARBOR™

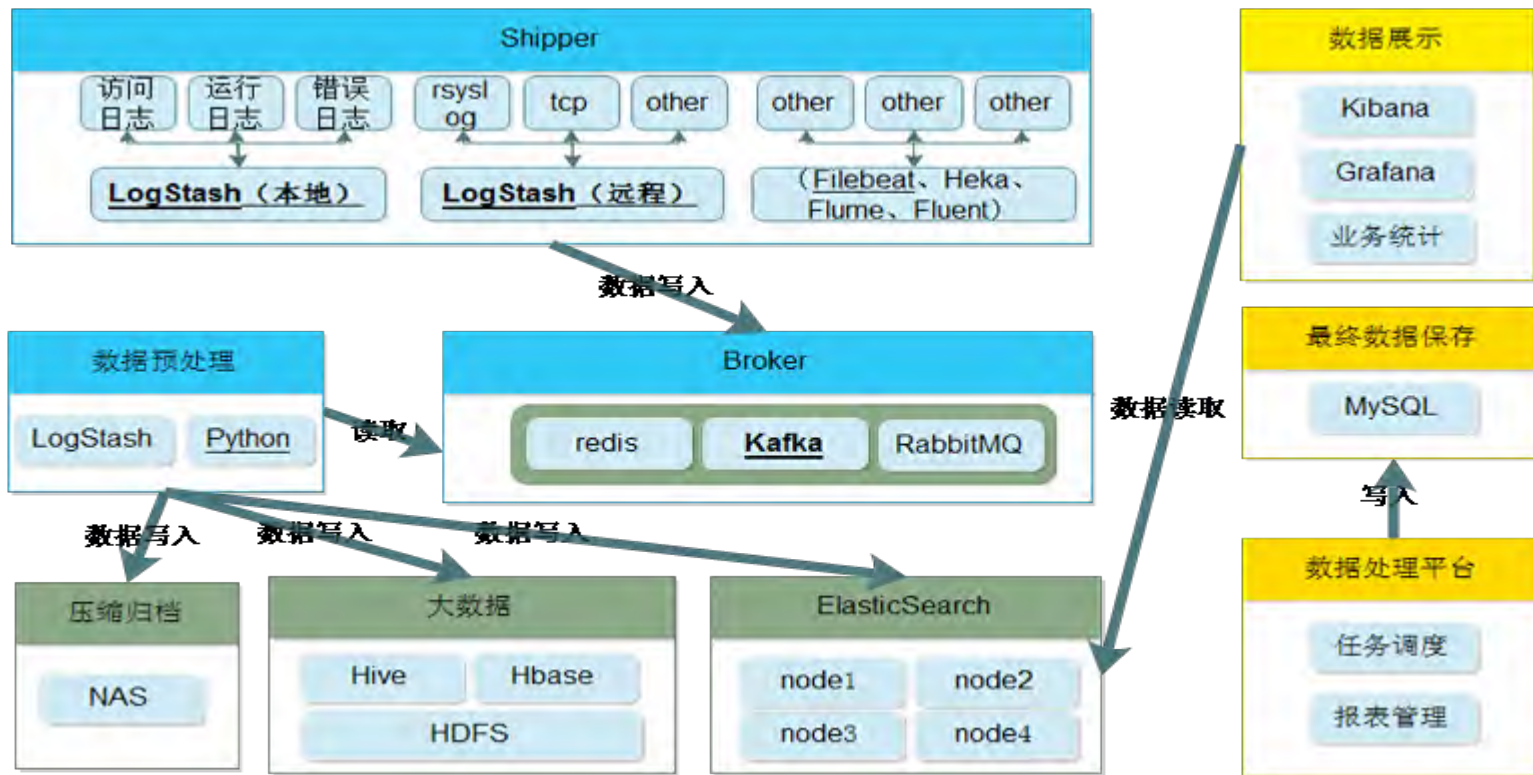


图片来自《高效运维社区》



GOPS2017
Beijing

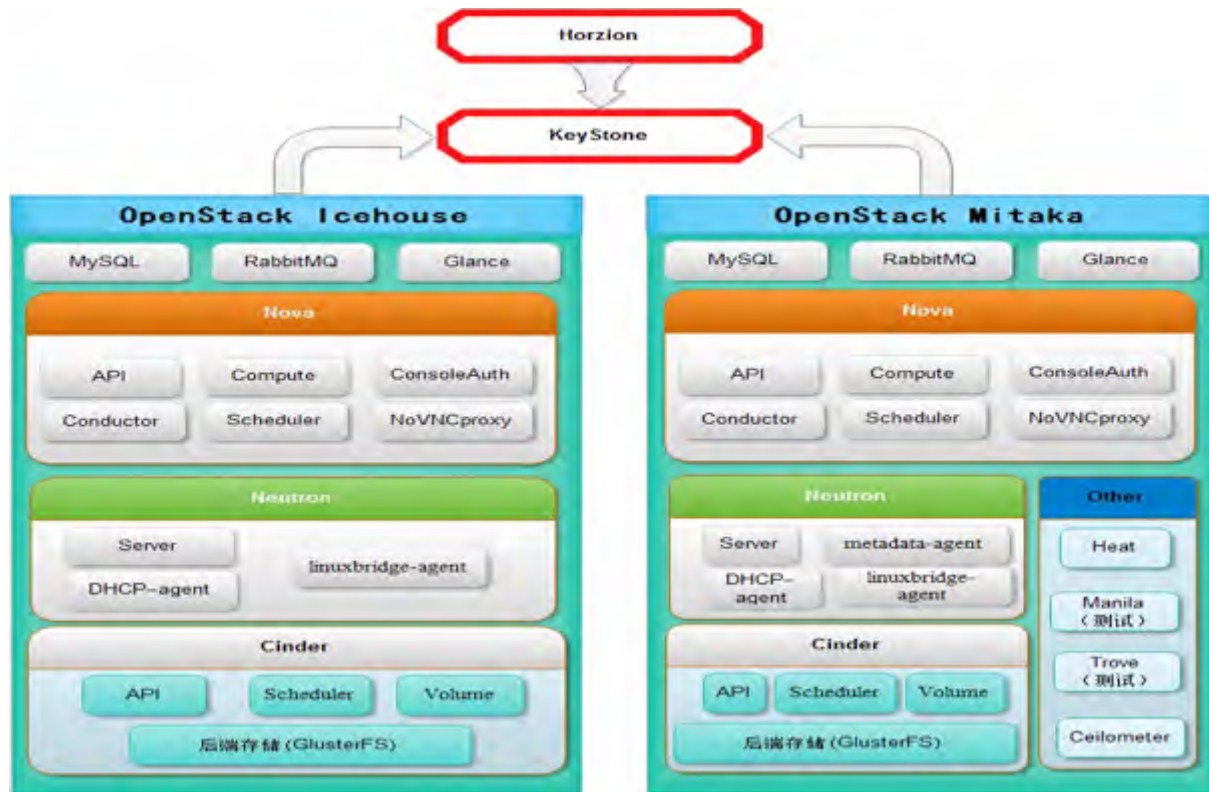
基于Elastic Stack的日志平台



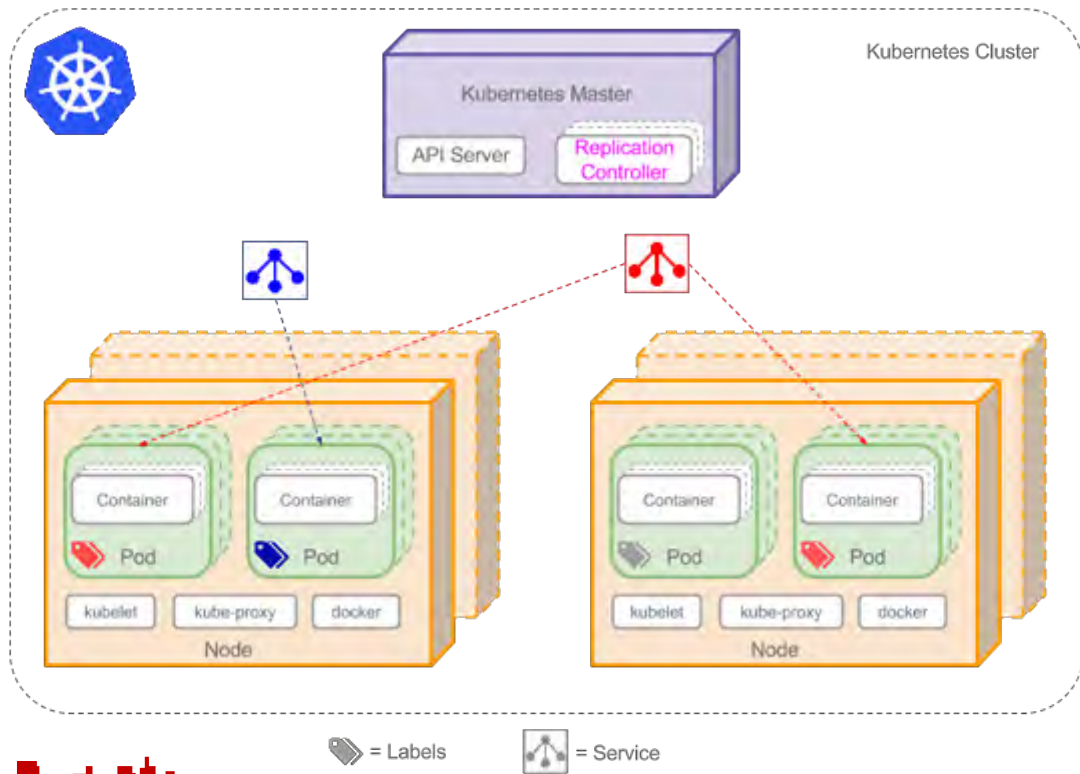
基于OpenStack构建企业私有云



GOPS2017
Beijing



基于Kubernetes构建容器平台



Kubernetes架构

- Pod
- Node
- Master
- Service



GOPS2017
Beijing

目录

1 基于开源的全链路自动化运维体系

➔ 2 Elastic Stack介绍

3 Elasticsearch入门

4 LogStash实战入门

5 架构解耦之消息队列

6 Kibana简介和企业实践



GOPS2017
Beijing

运维面临的困惑

开发：Hi，哥们，我刚才上线了一个功能，帮我看下运行日志有没有什么异常.....

运维：好的，马上

测试：Hi，兄弟，目前A接口的访问量掉了，帮我看下错误日志有啥ERROR.....

运维：好的，稍等

开发：Hi，好基友，帮我把我Log目录下的日志文件帮我取下来.....。

运维：好的，过会给你



日志的需求

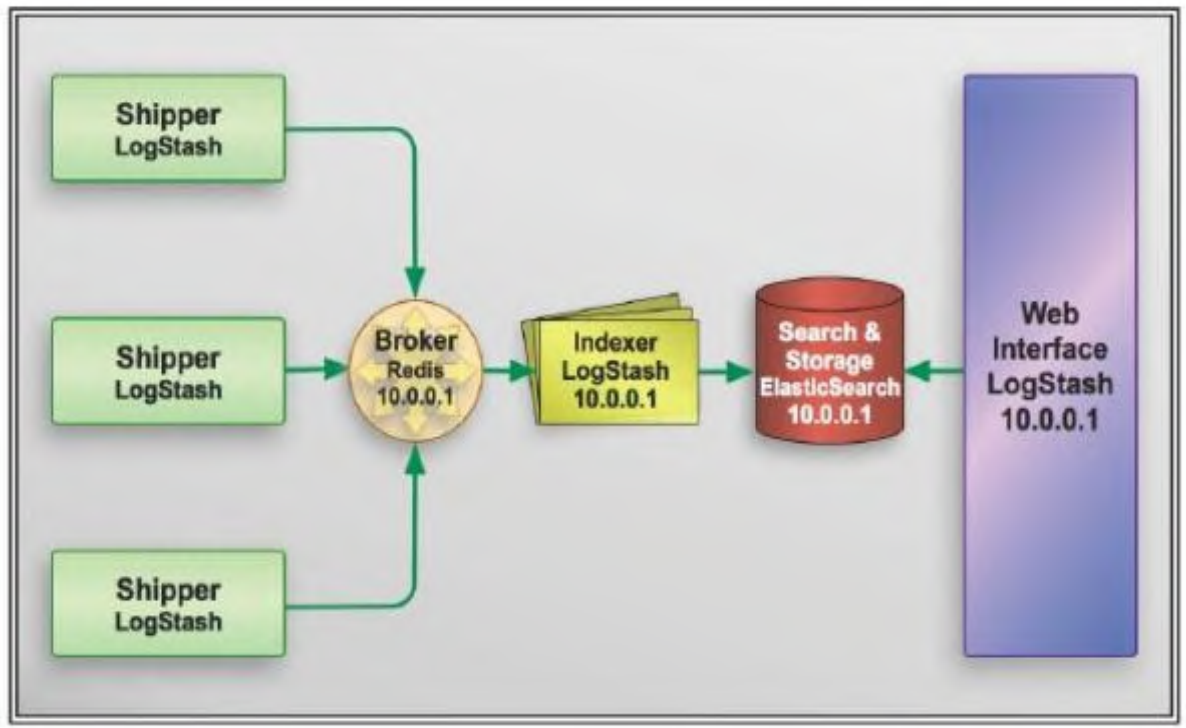
- 掌握操作系统的运行状况（系统日志）
- 统计分析如访问来源、URL访问频率、请求执行时间、成功率等（访问日志）
- 掌握应用运行中的详情、运行异常和业务日志输出（运行日志）
- 监控当前Web服务的运行情况，根据关键字查询日志详情（错误日志）
- 其它和系统或者业务相关的日志

环境的困境



- 开发人员不能登录线上服务器查看详细日志。
- 各个系统都有日志，日志数据分散难以查找。
- 日志数据量大，查询速度慢，或者数据不够实时。

曾经的ELK



ELK Stack

- Elasticsearch
- Logstash
- Kibana

Elasticsearch简介



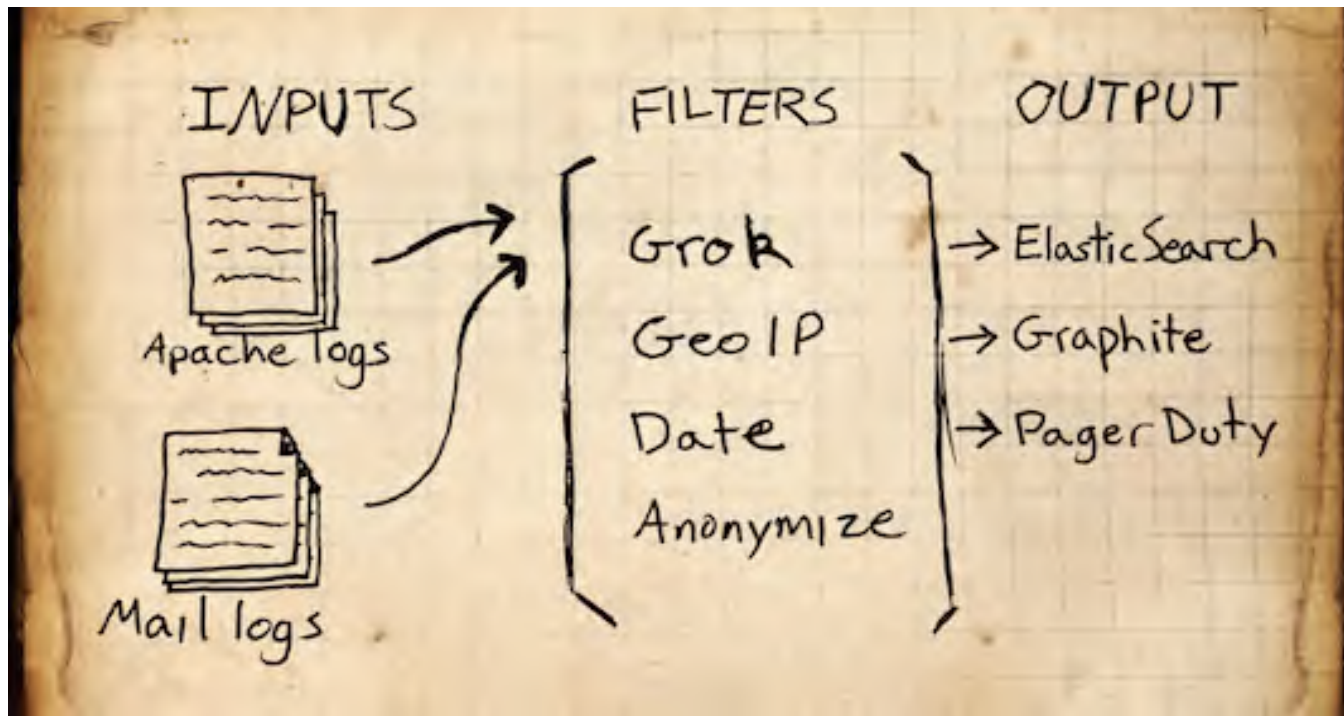
GOPS2017
Beijing

```
Elasticsearch  
curl -XPUT http://localhost:9200/twitter/tweet/1 -d '{  
  "user": "kimchy",  
  "post_date": "2009-11-15T13:12:00",  
  "ser": "kimchy", "message": "Trying out elasticsearch, so far so good?"  
  "ost_date": "200  
  "essage": "Tryin
```

LogStash简介



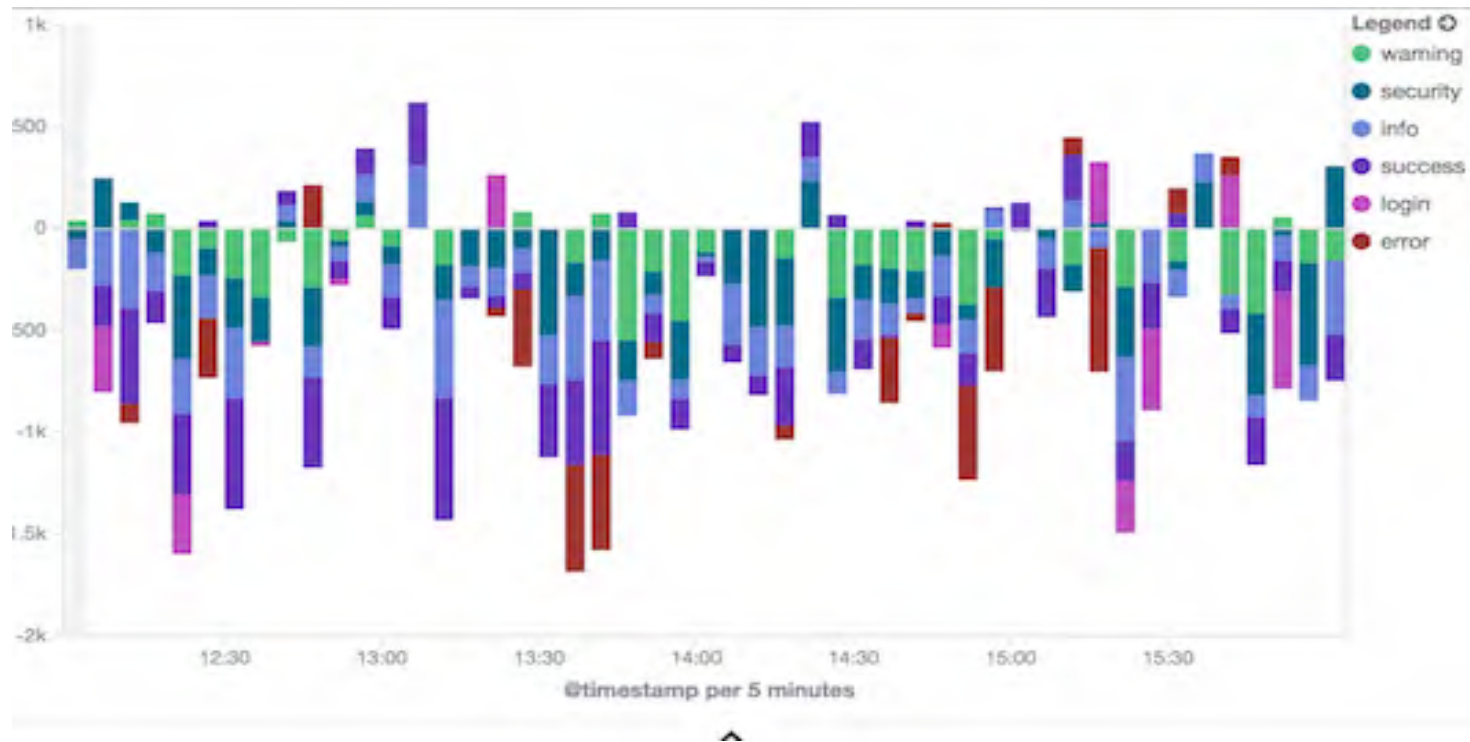
GOPS2017
Beijing



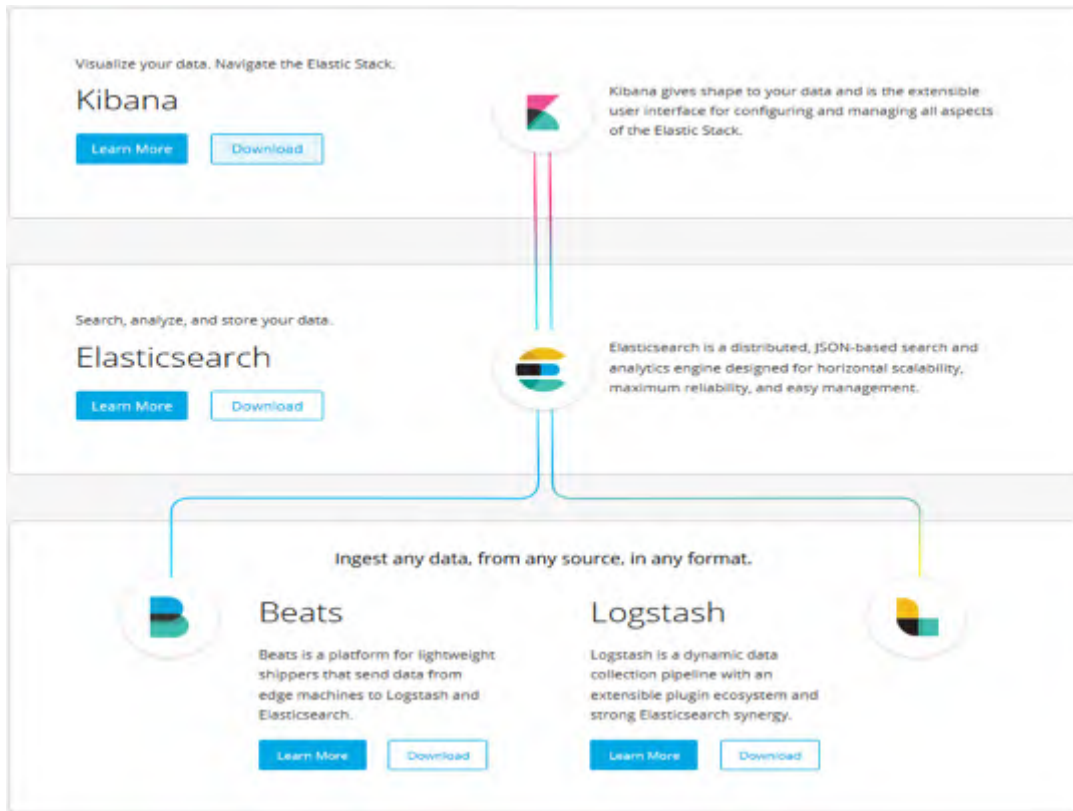
Kibana简介



GOPS2017
Beijing



现在的Elastic Stack



The Open Source Elastic Stack

- Kibana
- Elasticsearch
- Beats
- Logstash



GOPS2017
Beijing

目录

1 基于开源的全链路自动化运维体系

2 Elastic Stack介绍

➔ 3 Elasticsearch入门

4 LogStash实战入门

5 架构解耦之消息队列

6 Kibana简介和企业实践

与ElasticSearch交互



- Java API
- RESTful API with JSON over HTTP

```
curl -X<VERB> '<PROTOCOL>://<HOST>:<PORT>/<PATH>?<QUERY_STRING>' -d '<BODY>'
```

```
curl -XGET 'http://localhost:9200/_count?pretty' -d '{
  "query": {
    "match_all": {}
  }
}'
```

ElasticSearch集群状态



```
GET /_cluster/health
```

```
{
  "cluster_name":      "elasticsearch",
  "status":            "green", ❶
  "timed_out":         false,
  "number_of_nodes":   1,
  "number_of_data_nodes": 1,
  "active_primary_shards": 0,
  "active_shards":     0,
  "relocating_shards": 0,
  "initializing_shards": 0,
  "unassigned_shards": 0
}
```

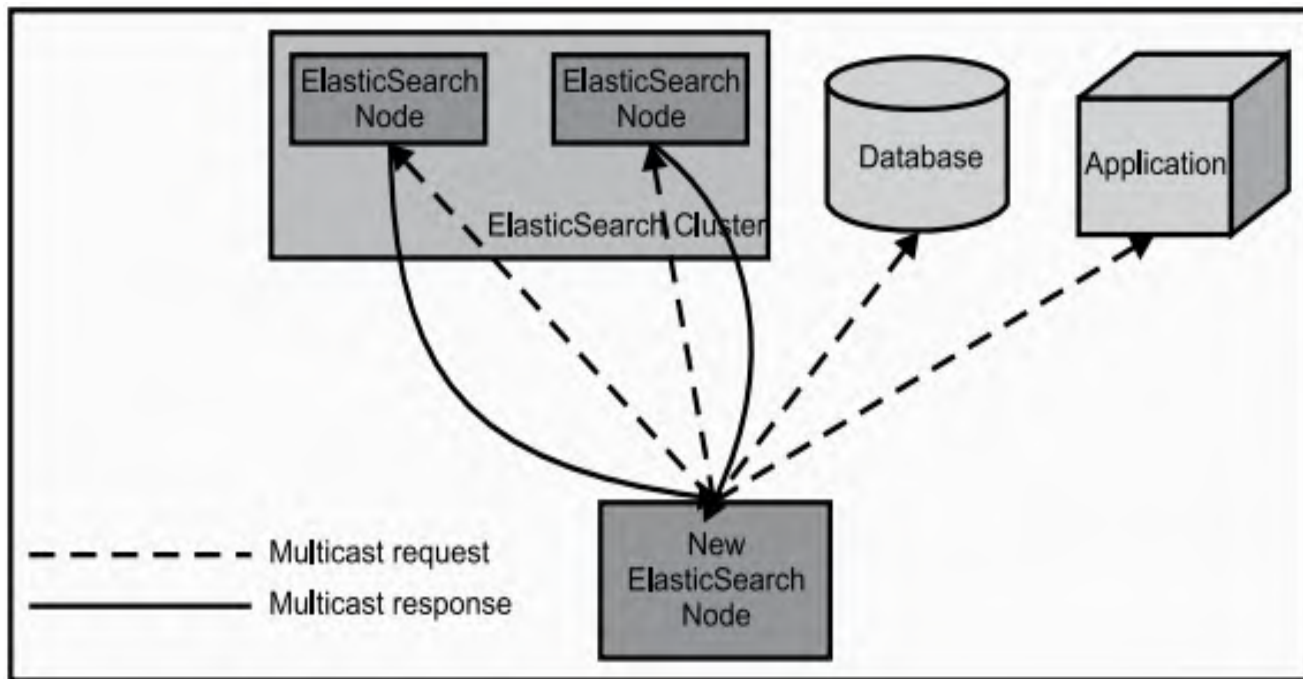
集群状态说明

- **green** 所有的主分片和副本分片都正常运行。
- **yellow** 所有的主分片都正常运行，但不是所有的副本分片都正常运行。
- **red** 有主分片没能正常运行。

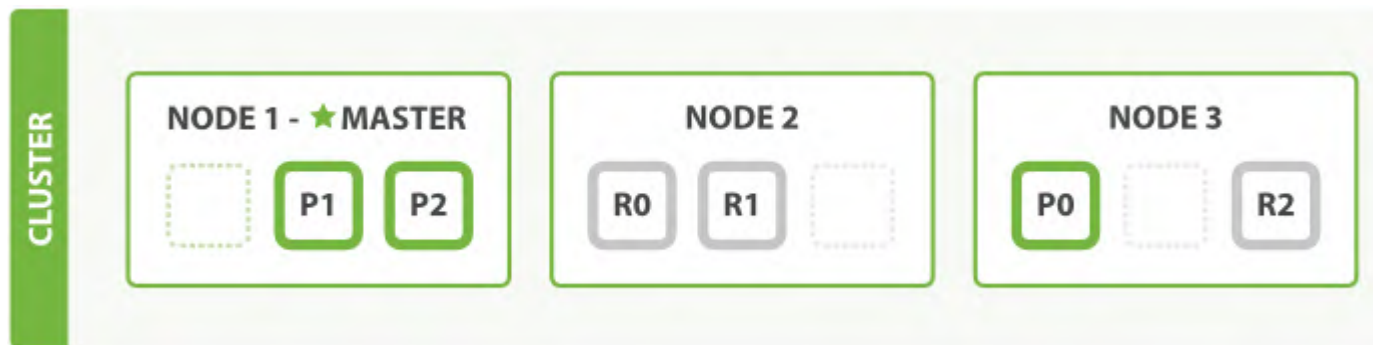
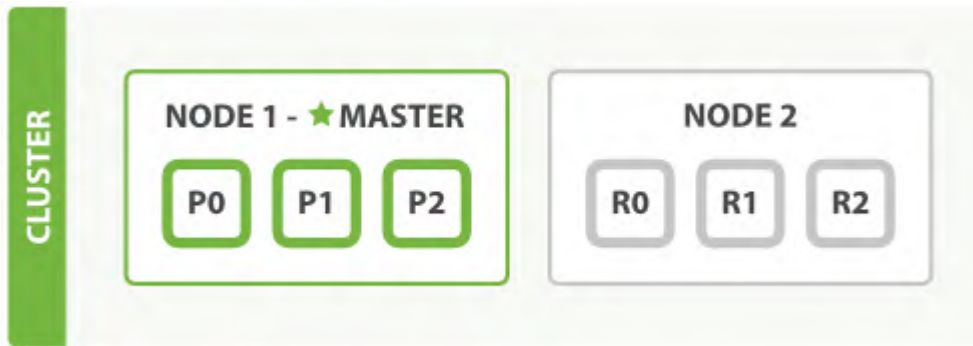
ElasticSearch集群发现：多播→单播



GOPS2017
Beijing



ElasticSearch集群增加节点





GOPS2017
Beijing

增加副本分片数量

```
PUT /blogs/_settings
{
  "number_of_replicas" : 2
}
```

将参数 `number_of_replicas` 调大到 2



有节点宕机？

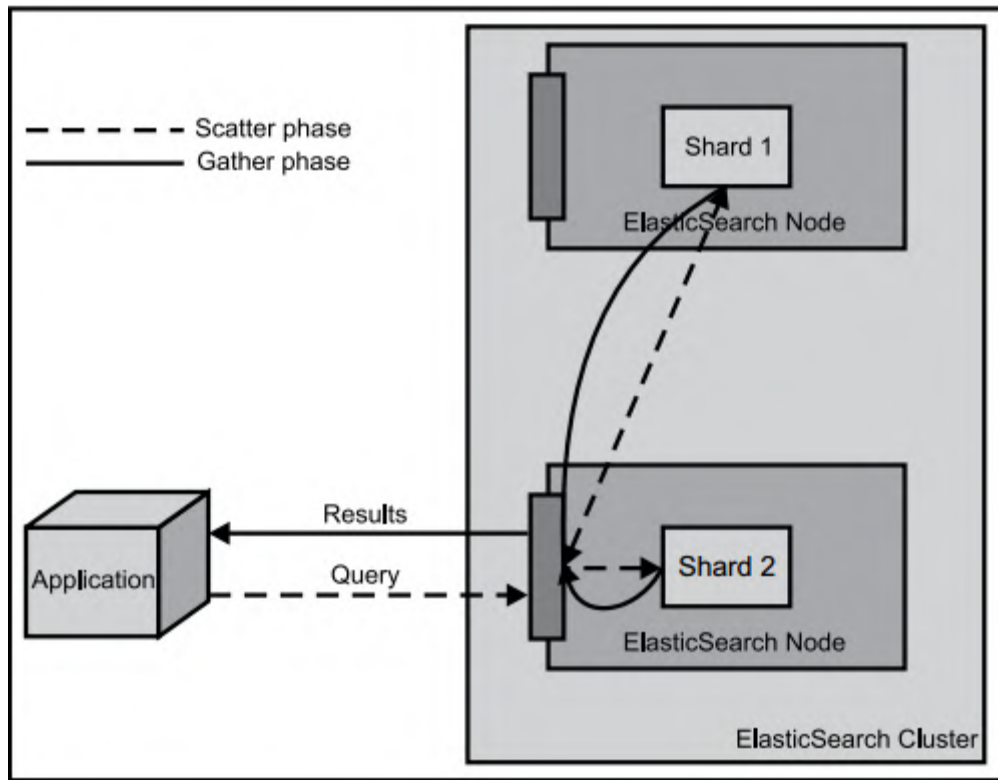


1. 如果是主节点宕机，会自动重新选举。
2. 分片自动平衡。

数据查询



GOPS2017
Beijing





GOPS2017
Beijing

目录

1 基于开源的全链路自动化运维体系

2 Elastic Stack介绍

3 Elasticsearch入门

➔ 4 LogStash实战入门

5 架构解耦之消息队列

6 Kibana简介和企业实践

LogStash的Hello world!



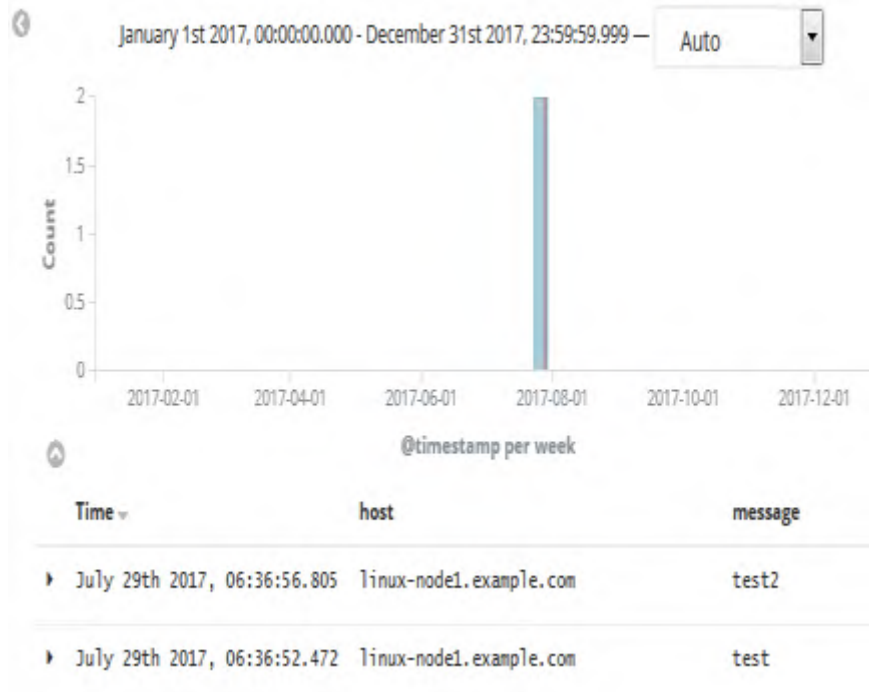
```
# logstash -e 'input { stdin { } } output { stdout { codec => rubydebug } }'
```

```
hello world
{
  "@timestamp" => 2017-07-28T21:35:12.879Z,
  "@version" => "1",
  "host" => "linux-node2.example.com",
  "message" => "hello world"
}
```

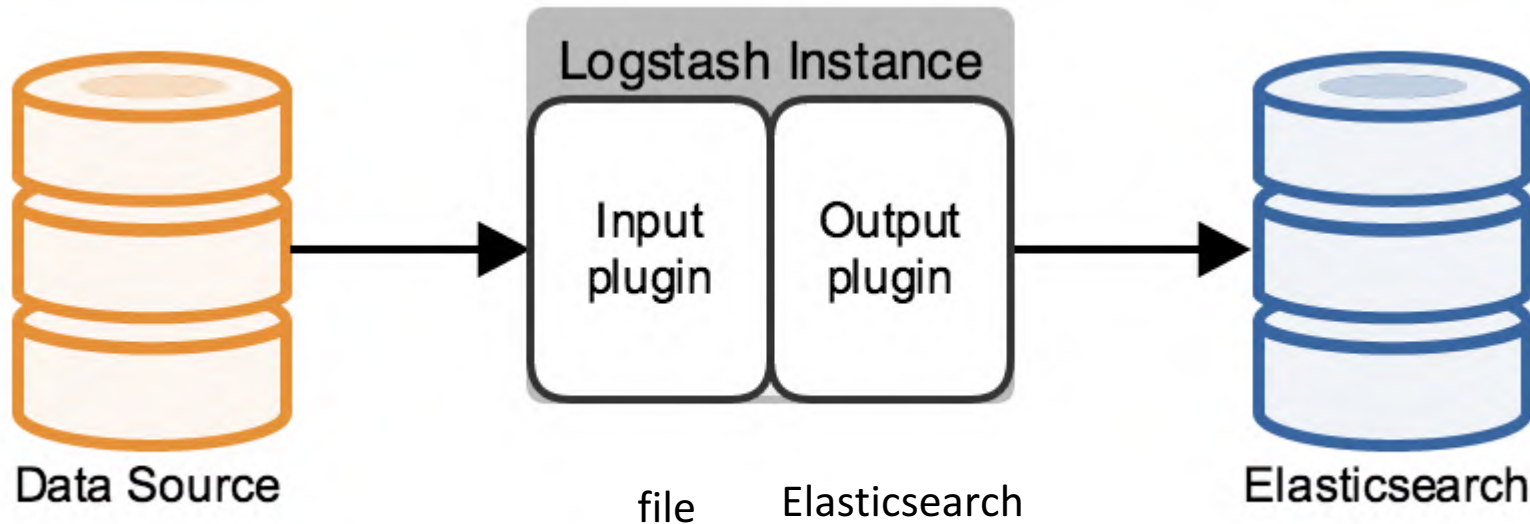
Output可以有多个



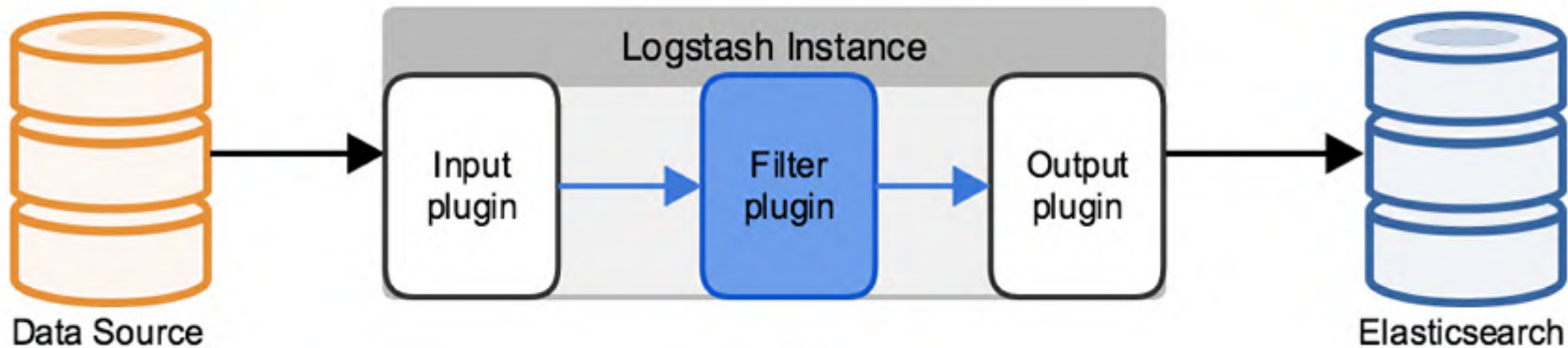
```
[root@linux-node1 ~]# cat demo.conf
input { stdin {} }
output {
  elasticsearch {
    hosts => ["192.168.56.11"]
  }
  stdout {
    codec => rubydebug
  }
}
```



LogStash Input+Output



LogStash Input + Filter + Output





GOPS2017
Beijing

目录

1 基于开源的全链路自动化运维体系

2 Elastic Stack介绍

3 Elasticsearch入门

4 LogStash实战入门

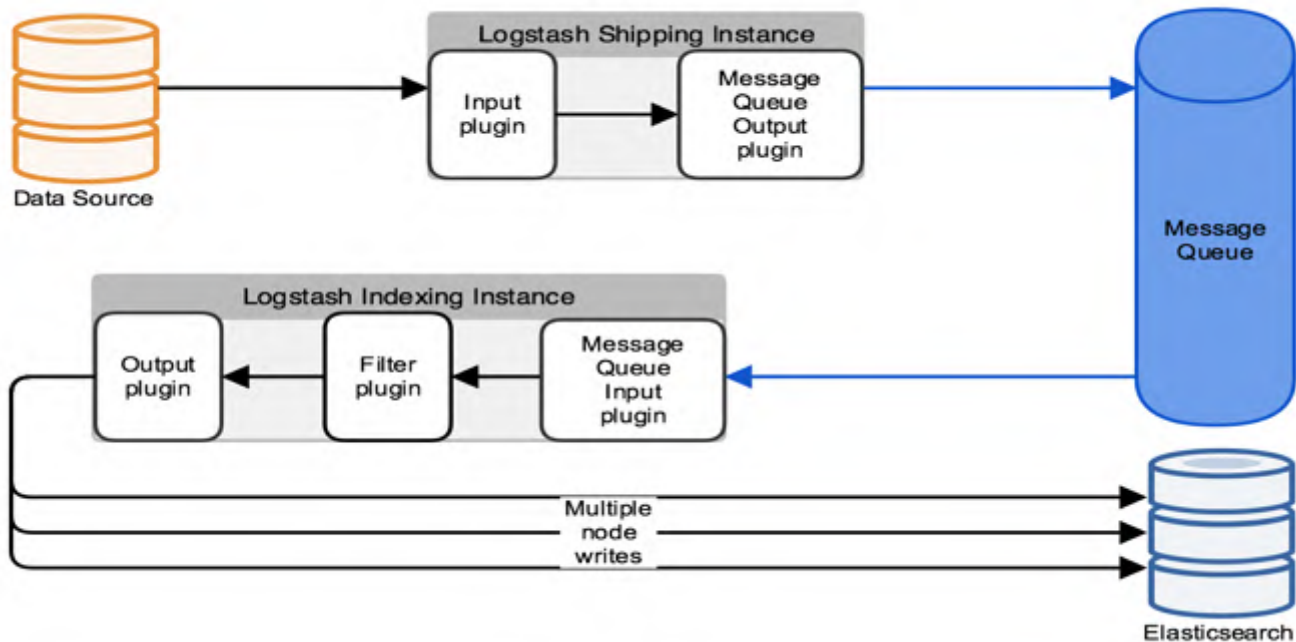
➔ 5 架构解耦之消息队列

6 Kibana简介和企业实践

使用消息队列



GOPS2017
Beijing



目录

1 基于开源的全链路自动化运维体系

2 Elastic Stack介绍

3 Elasticsearch入门

4 LogStash实战入门

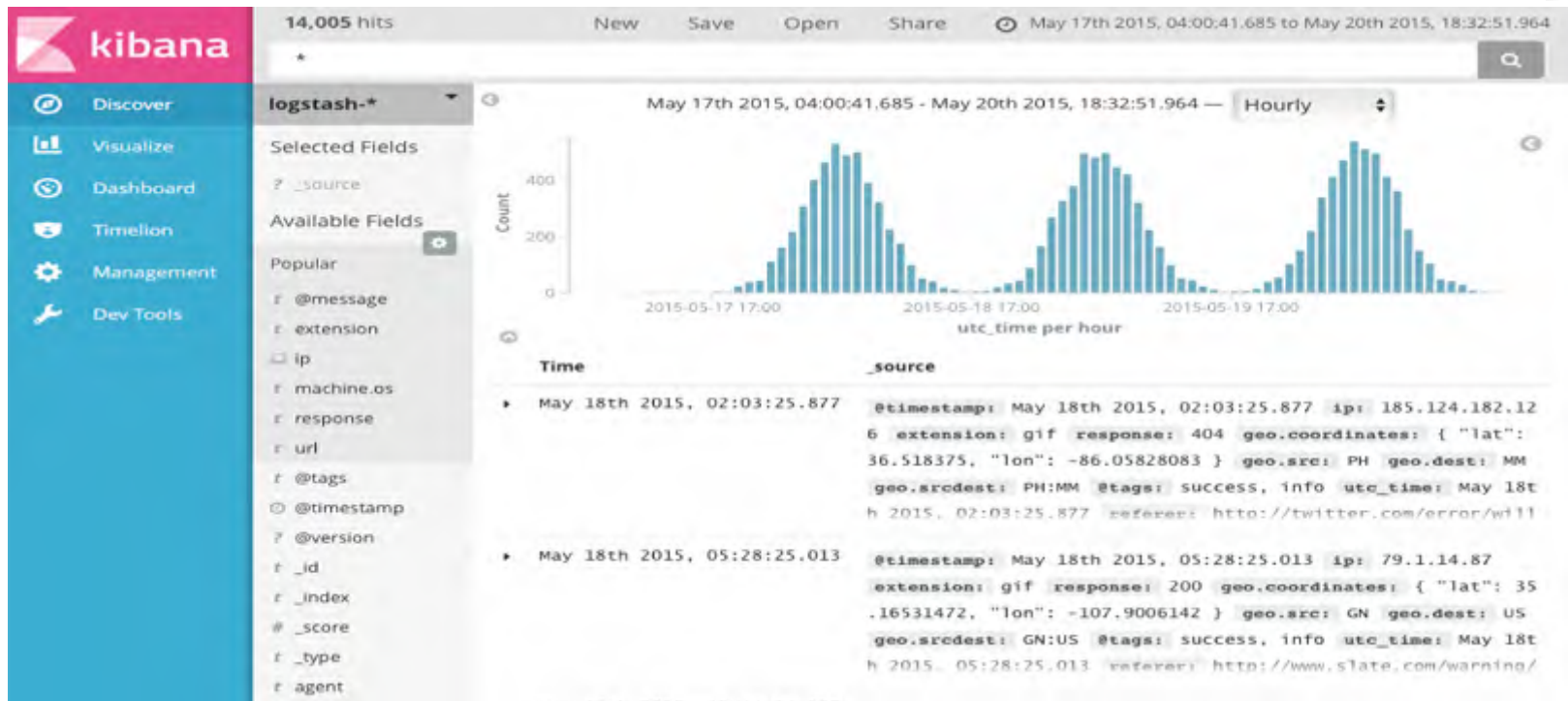
5 架构解耦之消息队列

➔ 6 Kibana简介和企业实践

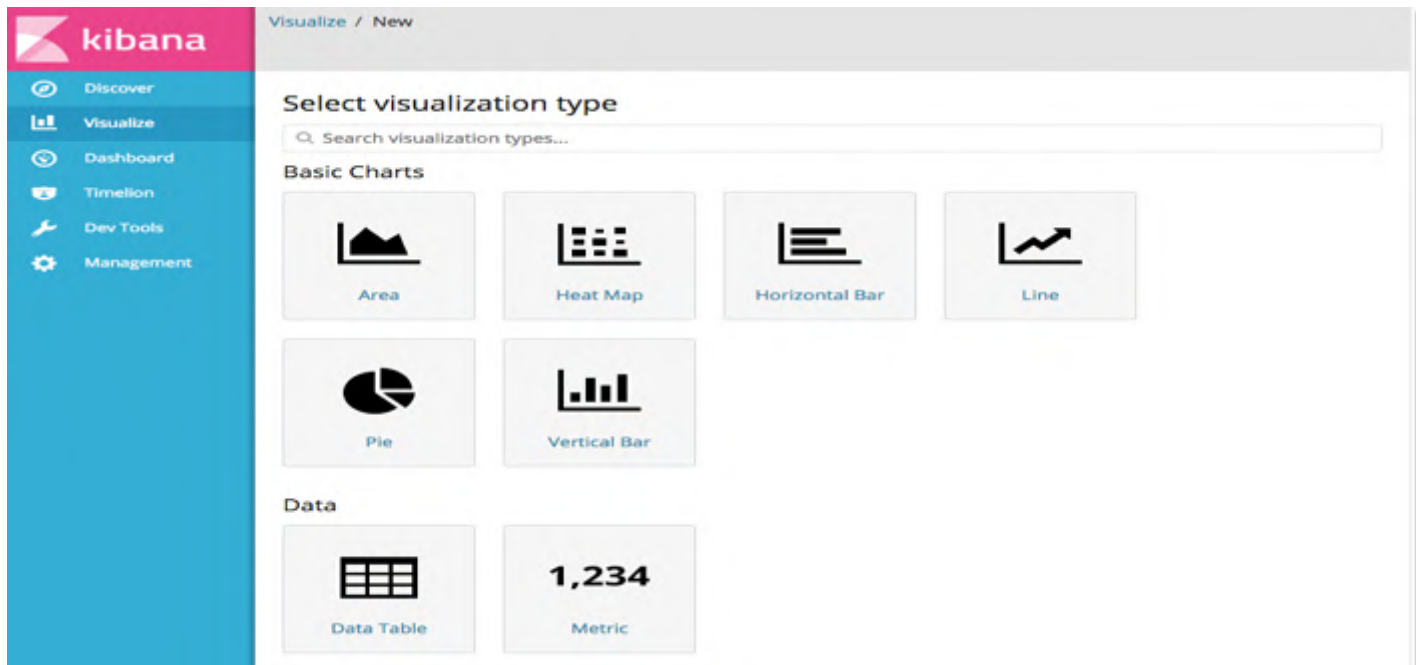
Kibana 5.x



GOPS2017
Beijing



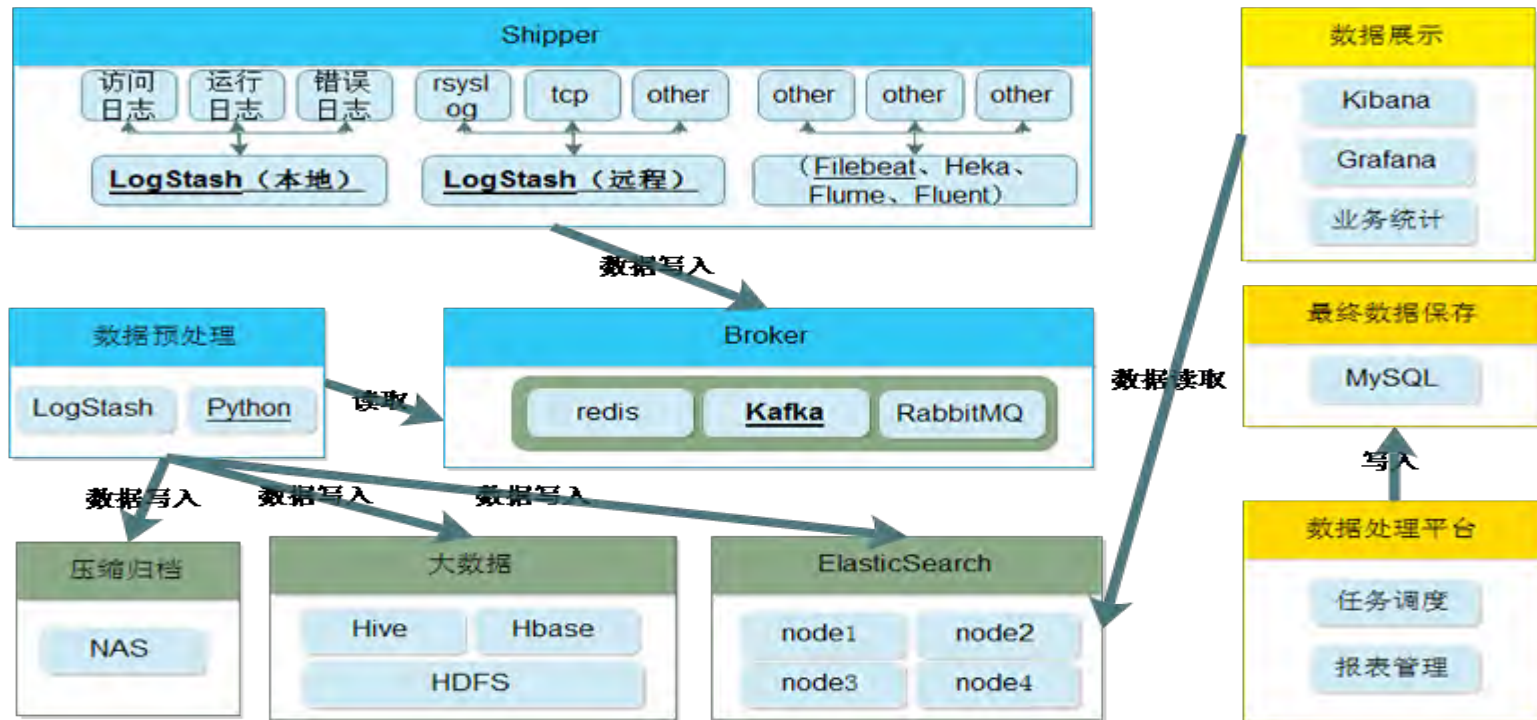
Kibana可视化图表





GOPS2017
Beijing

基于ELK的数据平台





GOPS2017
Beijing



企业DevOps运维专家

针对已经组建运维团队的企业

7x24运维值班监控服务
高级技术支持和顾问服务

针对还未组建运维团队的企业

7x24一站式运维托管服务
高性能Web架构规划与实施

自动化运维和DevOps解决方案

运维技术培训【云计算、自动化运维、Web架构】

通用基础服务



高效运维社区
GreatOPS Community



GOPS2017
Beijing

会议

- 8月18日 DevOpsDays 上海
- 全年 DevOps China 巡回沙龙
- 11月17日 DevOps金融上海

培训

- EXIN DevOps Master 认证培训
- DevOps 企业内训
- DevOps 公开课
- 互联网运维培训

咨询

- 企业DevOps 实践咨询
- 企业运维咨询



商务经理：刘静女士
电话 / 微信：13021082989
邮箱：liujing@greatops.com



GOPS2017
Beijing



Thanks

高效运维社区
开放运维联盟

荣誉出品



GOPS2017
Beijing



想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好

