

ELK在运维工作中应用两三事

上海安畅运维专家 韩军辉

场景一：数据中心流量分析

安畅网络背景介绍



面对的挑战和思考

挑战

单数据中心每秒最高10G+流量

单数据中心每月高达3000次DDOS

思考

流量数据的分析与展现

快速检查出DDOS攻击及异常流量

快速识别出攻击的线路、IP地址、对应客户信息等

数据中心流量全景

北艾机房流量全景视图

1

Q

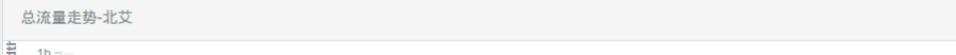
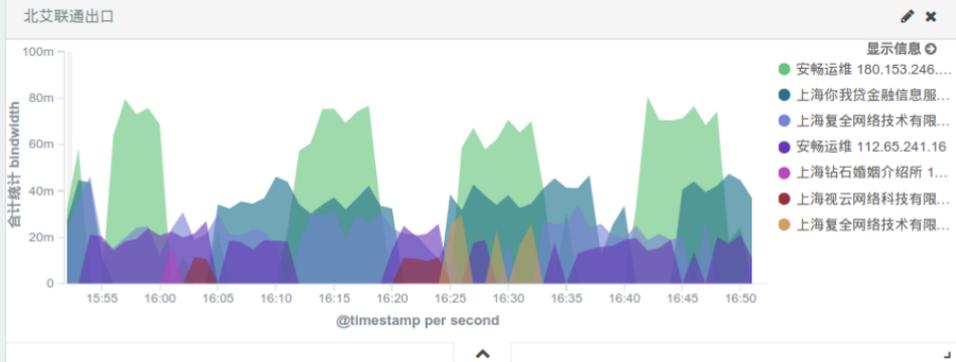
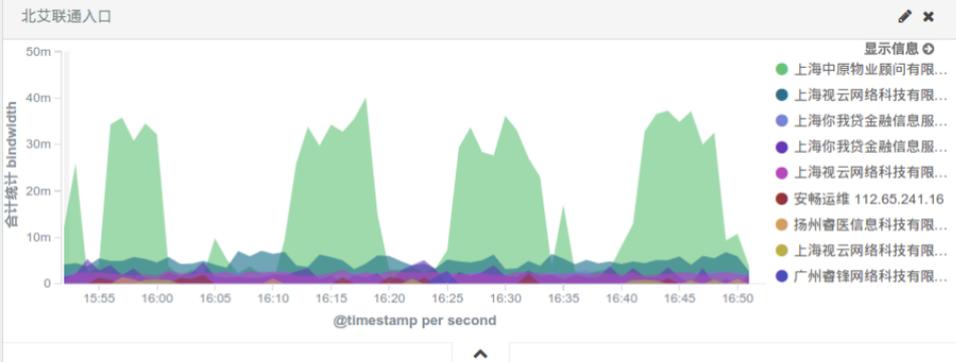
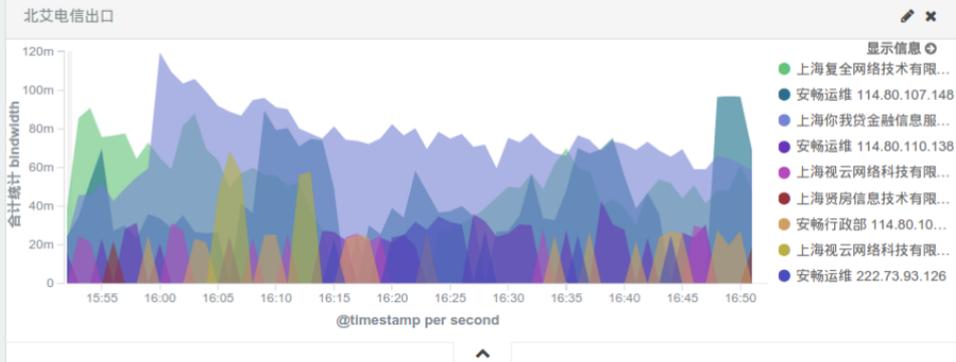
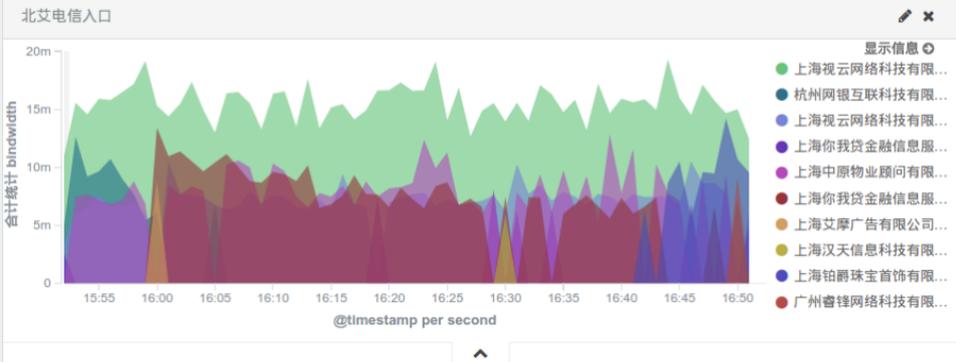
🔍

📄

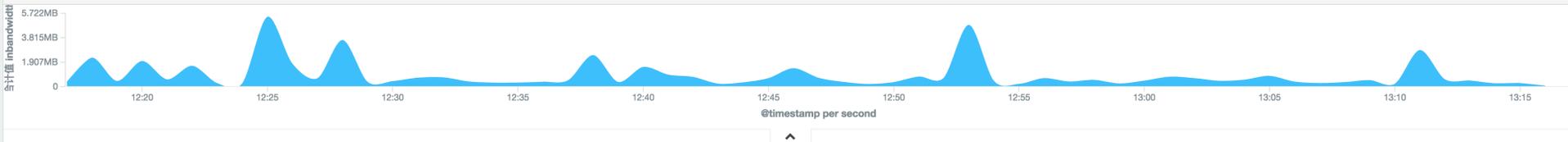
📁

🔗

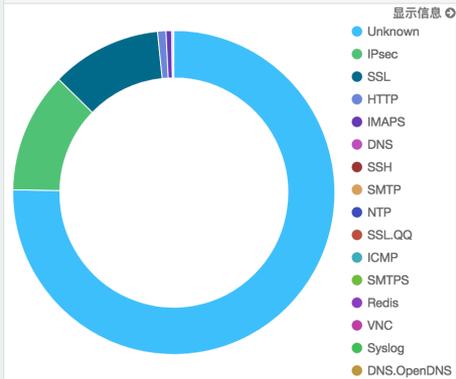
+



入口流量走势



应用层协议分布



访问流量最多的地区



传输层协议分布



入口运营商统计



入口总流量



进入流量最多的来源IP

Top 10 IPV4_SRC_ADDR ⇅ Q	合计值 inbytes ⇅
118.193.144.4	84.162MB
221.228.82.34	54.36MB
101.227.66.81	48.933MB
117.121.25.6	36.8MB

访客来源地热点图-flow



DDOS攻击告警

当前时间：2015-08-11 09:46

电信

联通

BGP

移动



3.1%

金海

北京云普互动信息技术有限公司
114.80.201.18 0.4%
南京奋斗网络科技有限公司
114.80.203.84 0.4%
上海广升信息技术有限公司
114.80.203.122 0.4%
南京奋斗网络科技有限公司
114.80.201.77 0.2%
上海安畅网络有限公司
114.80.201.30 0.2%



2.4%

昆山

吉林省高升科技有限公司
180.97.80.148 0.3%
合肥企云呼信息科技有限公司
180.97.81.43 0.2%
合肥企云呼信息科技有限公司
180.97.81.100 0.2%
上海联网科贸有限公司
180.97.70.113 0.2%
北京数字狗狗网络技术有限公司(原李福)
180.97.69.8 0.2%



24.1%

南汇

深圳市亚速维亿科技有限公司
222.73.216.145 10.5%
上海菲通信服务有限公司
222.73.121.114 2.9%
江苏大圆银泰商品合约交易市场有限公司
222.73.107.40 2.4%
红槎(上海)快递有限公司
222.73.113.84 1.2%
上海傲林软件技术有限公司
222.73.216.253 0.8%



4.8%

北艾

上海视云网络科技有限公司
114.80.0.62 0.6%
上海中原物业顾问有限公司
114.80.110.198 0.6%
上海普景信息科技有限公司
114.80.88.46 0.4%
上海比邻美车美容有限公司
114.80.110.211 0.4%
上海视云网络科技有限公司
114.80.0.43 0.4%



1.2%

无锡

网宿科技股份有限公司(福建)
58.215.139.25 0.1%
杭州网银互联科技有限公司
221.228.197.226 0.1%
网宿科技股份有限公司(福建)
221.228.197.26 0.1%
网宿科技股份有限公司(福建)
221.228.197.22 0.1%
网宿科技股份有限公司(上海)
58.215.142.33 0.1%



3%

呼兰

艾扬软件(上海)有限公司
103.36.132.242 0.6%
阳光雨露信息技术服务(北京)有限公司
103.6.222.59 0.6%
上海嘉之道企业管理咨询有限公司
101.227.71.170 0.2%
上海联智信息科技发展有限公司
101.227.78.162 0.2%
thinkxen 103.20.248.192 0.1%



0.4%

金桥

宁夏汇银白银交易中心有限公司
180.153.246.124 0.4%



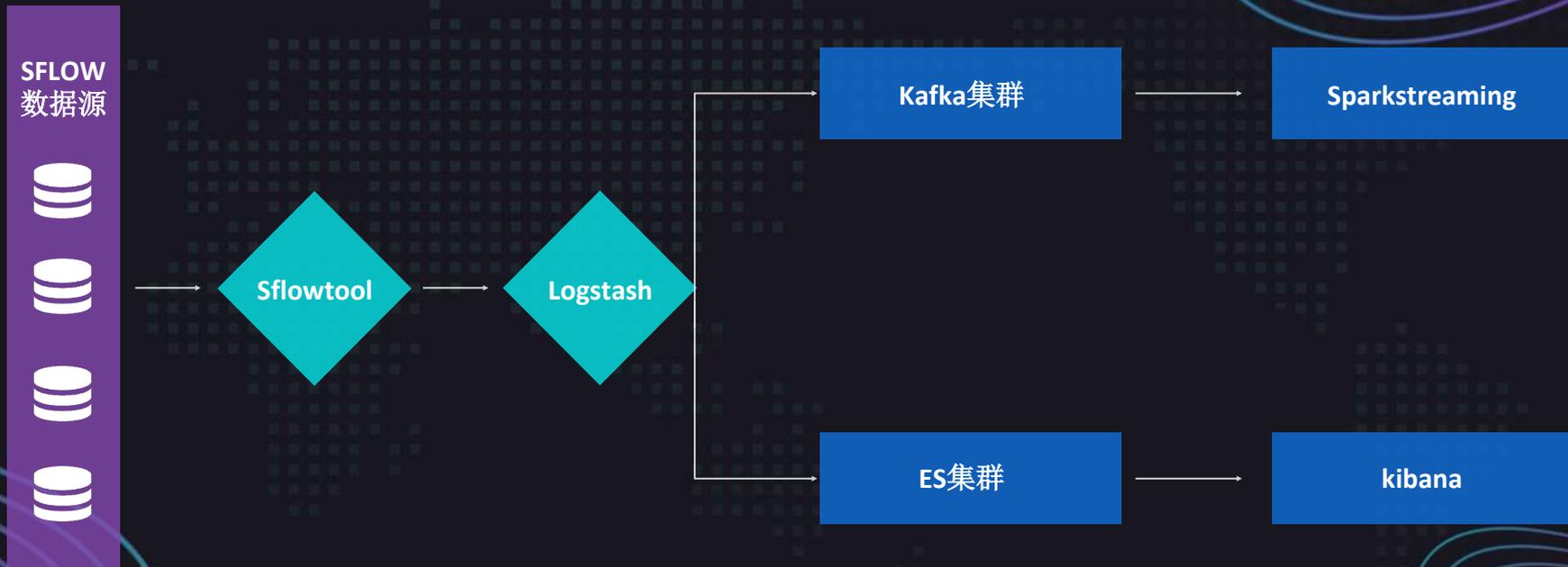
0.1%

长沙

CYCOM HONG KONG LIMITED
124.232.150.226 0.0%
CYCOM HONG KONG LIMITED
124.232.163.84 0.0%
江苏汇众网络科技有限公司
175.6.128.203 0.0%
CYCOM HONG KONG LIMITED
124.232.163.104 0.0%
江苏汇众网络科技有限公司
124.232.148.97 0.0%

TIME	DATA CENTER	AGENT IP	PERCENT	CUSTOMER
2015-08-18 16:11:24	长沙	124.232.137.153	16.81%	CYCOM HONG KONG LIMITED 124.232.163.120
2015-08-18 16:11:24	无锡	58.215.171.6	10.33%	吉林省高升科技有限公司 103.21.119.5
2015-08-18 16:11:24	怒江	117.135.137.81	10.35%	CYCOM HONG KONG LIMITED 221.181.64.40
2015-08-18 16:11:24	昆山	180.97.70.3	10.27%	合肥企云呼信息科技有限公司 180.97.81.100
2015-08-18 16:11:24	鲁谷	124.202.141.9	12.36%	恒拓开源(天津)信息科技股份有限公司 211.155.89.196
2015-08-18 16:11:24	鲁谷	124.202.141.9	21.42%	上海视云网络科技有限公司 124.202.157.13
2015-08-18 16:11:24	南汇	222.73.124.237	13.62%	上海菲通信服务有限公司 114.141.132.130
2015-08-18 16:11:24	长沙	124.232.137.153	11.41%	江苏汇众网络科技有限公司 175.6.128.202
2015-08-18 16:11:24	北艾	222.73.184.128	14.50%	上海中原物业顾问有限公司 114.80.110.198
2015-08-18 16:11:24	鲁谷	124.202.141.9	15.57%	上海五帝科技有限公司 124.202.157.35
2015-08-18 16:11:24	无锡	58.215.171.6	11.69%	吉林省高升科技有限公司 103.21.119.7

技术架构



```
sFlow Version 5 Information:
```

```
-----  
Agent Information:
```

```
    IP Address: 103.6.222.106  
Address family: IPV4  
vpn-instance: NA
```

```
-----  
Collector Information:
```

```
Collector ID: 1  
  IP Address: 58.219.179.152  
Address family: IPV4  
vpn-instance: NA  
  Port: 2065  
Datagram size: 1400  
  Time out: NA  
Description: sflow
```

```
Collector ID: 2  
  IP Address: 221.228.82.88  
Address family: IPV4  
vpn-instance: NA  
  Port: 6352  
Datagram size: 1400  
  Time out: NA  
Description: JiDanTu
```

```
-----  
Port on slot 1/5 Information:
```

关键配置

```
Interface: XGE1/6/0/3
Flow-sample collector: NA          Counter-sample collector : 1,2
Flow-sample rate(1/x): 512       Counter-sample interval(s): 2
Flow-sample maxheader: 128
Flow-sample direction: IN,OUT
```

 Port on slot 2/5 Information:

Port on slot 2/6 Information:

```
Interface: XGE2/6/0/5
Flow-sample collector: NA          Counter-sample collector : 1,2
Flow-sample rate(1/x): 512       Counter-sample interval(s): 2
Flow-sample maxheader: 128
Flow-sample direction: IN,OUT
```

- "114.80.200.1": 安畅运维
- "114.80.200.2": 上海信通网络科技有限公司
- "114.80.200.3": 上海信通网络科技有限公司
- "114.80.200.4": 上海信通网络科技有限公司
- "114.80.200.5": 上海信通网络科技有限公司
- "114.80.200.6": 上海信通网络科技有限公司
- "114.80.200.7": 上海信通网络科技有限公司
- "114.80.200.9": 安畅运维
- "114.80.200.10": 上海信通网络科技有限公司
- "114.80.200.11": 安畅运维

关键配置

```
input {  
    pipe {  
        type => "sflow"  
        command => "/var/scripts/sflowtool-wrapper.sh -l -p 6343"  
    }  
    pipe {  
        type => "sflow"  
        command => "/var/scripts/sflowtool-wrapper.sh -l -p 6344"  
    }  
    pipe {  
        type => "sflow"  
        command => "/var/scripts/sflowtool-wrapper.sh -l -p 6345"  
    }  
}
```

关键配置

```
filter {
  ## Sflow Monitor
  if "sflow" == [type] {
    grok {
      match => [ "message", "%{WORD},%{IP:Agent_address},%{NUMBER:In_
Port},%{NUMBER:Out_Port},%{DATA:Src_MAC},%{DATA:Dst_MAC},%{DATA:ethernet_type},%{NUMB
ER:in_vlan},%{NUMBER:out_vlan},%{IP:Src_IP},%{IP:Dst_IP},%{NUMBER:IP_protocol},%{DATA
:ip_tos},%{NUMBER:ip_ttl},%{NUMBER:Src_Port},%{NUMBER:Dst_Port},%{DATA:Tcp_flags},%{I
NT:packet_size:int},%{NUMBER:IP_size},%{NUMBER:sampling_rate}" ]
    }
    translate {
      field => "IP_protocol"
      destination => "protocols"
      dictionary_path => "/home/translate/protocol"
      refresh_interval => 86400
    }
    translate {
      field => "Src_IP"
      destination => "customer"
      dictionary_path => "/home/translate/customerip"
      refresh_interval => 86400
      add_field => { "sfully" => "%{customer} %{Src_IP}" }
    }
    translate {
      field => "Dst_IP"
      destination => "customer"
      dictionary_path => "/home/translate/customerip"
      refresh_interval => 86400
    }
  }
}
```

场景二：日志分析和性能监控

为什么需要日志收集

- 掌握操作系统的运行状况
- 掌握应用运行中的详情、运行异常和业务日志输出
- 监控当前web服务的运行情况，根据关键字查询日志详情
- 等级保护的需要
-

过去的困境

- 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，查找困难并且效率低下
- 磁盘空间不足删除了日志
- 没有实时监控、分析
- 无法提供全文搜索
-

kibana

51,172 hits
New Save Open Share < Last 1 hour >

Use lucene query syntax

+
Add a filter

2018-01-10 15:05:01 - 2018-01-10 16:05:01
Auto

Time

_source

2018-01-10 16:04:59

```

                    message: {"log":"order renew finish order_title:eip\n","stream":"stdout","attrs":{"image":"service-order"},"time":"2018-01-10T08:04:59.89026967Z"} @version: 1
                    @timestamp: 2018-01-10 16:05:00 host: mesos-slave106 stream: stdout time: 2018-01-10 16:04:59 service_name: service-order container_id: f333158f5bde8a4b3b87135cfd44a7f3ed882d1e311652ceba75c0c2f387135 app_env: prod _id: AWFdGdaER4g13FQDJ-S9 _type: logs _index: docker-service-order-2018.01 _score: -
                
```

Table

JSON

[View surrounding documents](#)
[View single document](#)

@timestamp	Q Q	*	2018-01-10 16:05:00
@version	Q Q	*	1
_id	Q Q	*	AWFdGdaER4g13FQDJ-S9
_index	Q Q	*	docker-service-order-2018.01
#_score	Q Q	*	-
_type	Q Q	*	logs
app_env	Q Q	*	prod
container_id	Q Q	*	f333158f5bde8a4b3b87135cfd44a7f3ed882d1e311652ceba75c0c2f387135
host	Q Q	*	mesos-slave106 服务运行的主机
message	Q Q	*	{"log":"order renew finish order_title:eip\n","stream":"stdout","attrs":{"image":"service-order"},"time":"2018-01-10T08:04:59.89026967Z"}
service_name	Q Q	*	service-order 服务名称
stream	Q Q	*	stdout
time	Q Q	*	2018-01-10 16:04:59

Discover
Visualize
Dashboard
Timelion
Dev Tools
Monitoring
Management

Field	Value
@timestamp	2017-12-01 23:59:59
_id	AWASzLY-MSYQLkgNxbo3
_index	packetbeat-mysql-2017.12
_score	-
_type	mysql
beat.hostname	mysql-master
beat.name	mysql-master
beat.version	5.4.0
# bytes_in	472
# bytes_out	14
# client_ip	192.168.9.8
client_port	50387
client_proc	
client_server	
direction	in
ip	192.168.9.32
method	INSERT
# mysql.affected_rows	1
# mysql.error_code	0
mysql.error_message	
mysql.insert_id	605501
@ mysql.iserror	false
mysql.num_fields	0
mysql.num_rows	0
path	
port	3306
proc	
query	insert into Res_SysEmail(Title,EmType,Content,TemplateId,addResSee,BccEmail,RegularlySentTS,SentId,CreateUserId,CreateTs,isSend,CcEmail,OrderId,CustomerId,FailedSendem) values ('机柜分配状态异常 (机柜是未分配状态但有分配记录','noreply','Id:1048机柜编号: I04-br/>Id:8718机柜编号: I08-br/>Id:13666机柜编号: J08-br/>',null,'wangcq@51idc.com;chengll@51idc.com',null,'2017-12-2 0:0:0',null,1,'2017-12-2 0:0:0',1,null,null,null,null)
# responsetime	0

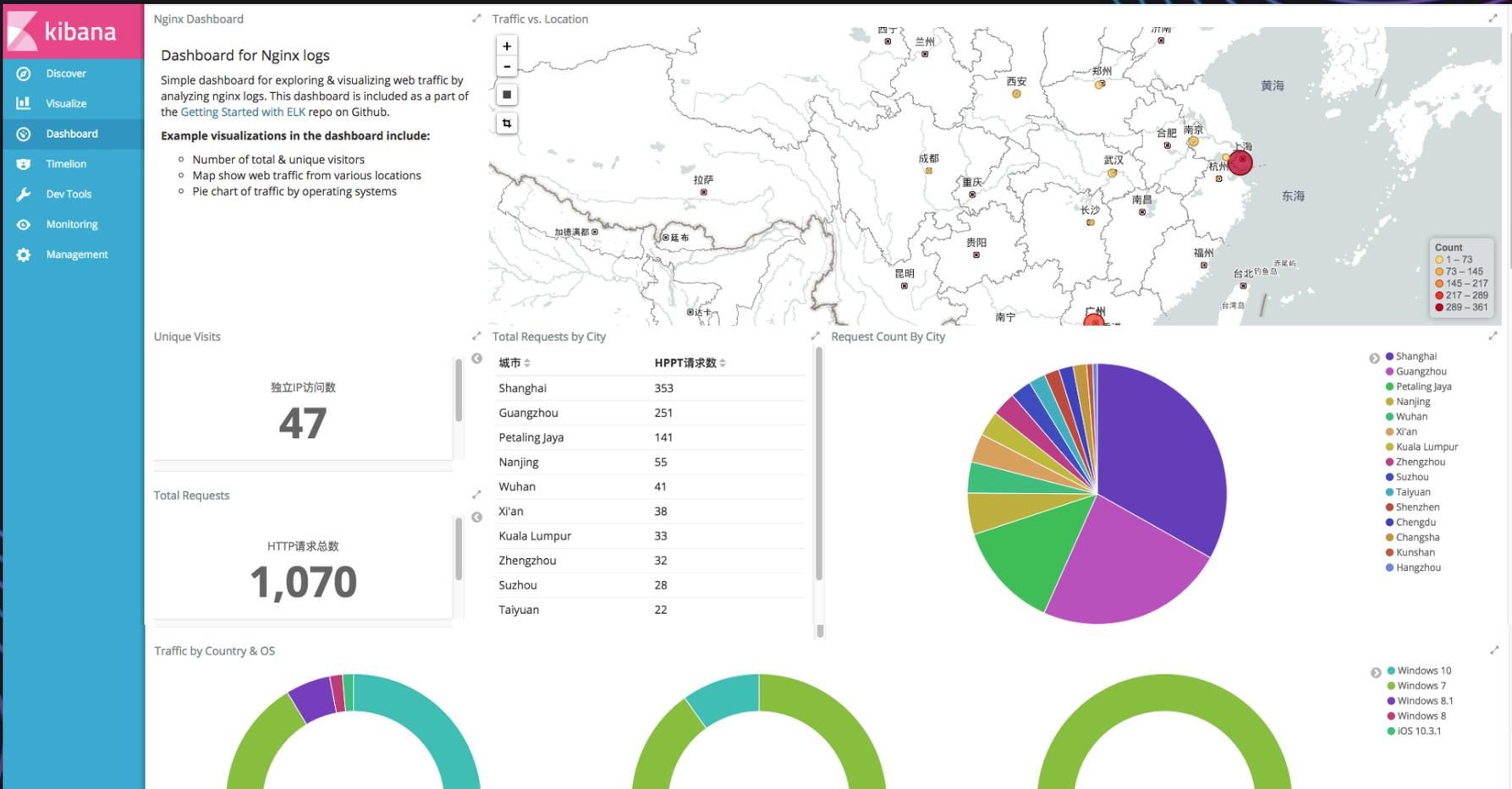
View surrounding documents View single document

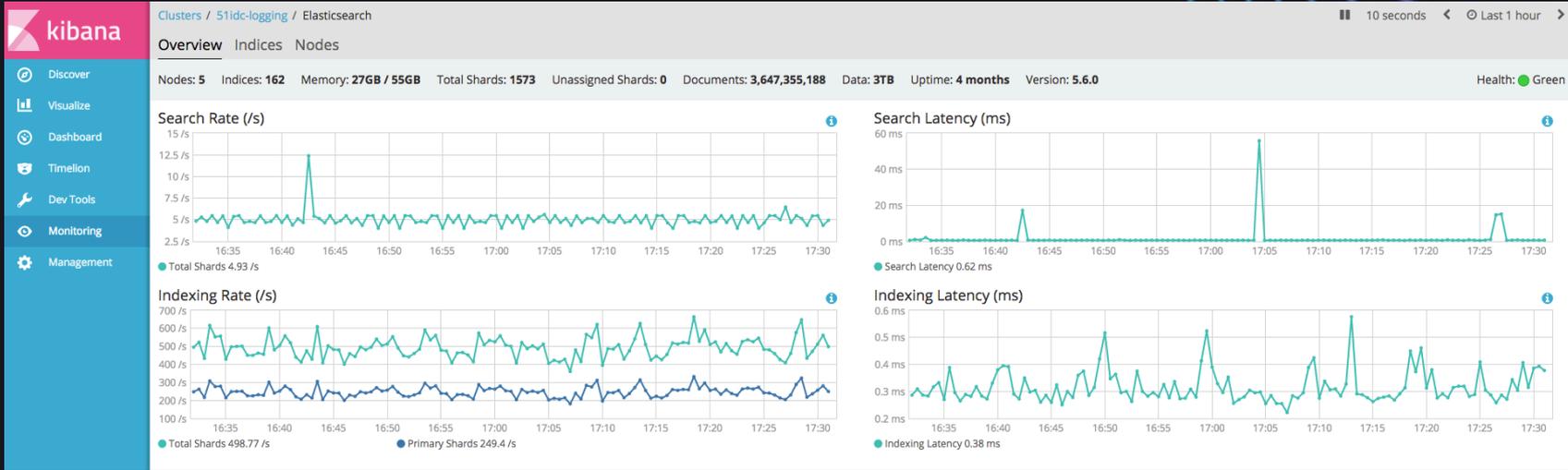
执行客户端

MySql主机ip

执行语句

Collapse





Clusters / 51idc-logging / Elasticsearch

Overview Indices Nodes

Nodes: 5 Indices: 162 Memory: 27GB / 55GB Total Shards: 1573 Unassigned Shards: 0 Documents: 3,647,358,014 Data: 3TB Uptime: 4 months Version: 5.6.0 Health: ● Green

Indices 20 of 145 Show system indices

Name	Status	Document Count	Data	Index Rate	Search Rate
docker-service-order-2017.09	● Green	22.4m	12.2 GB	0 /s	0 /s
webui	● Green	0	1.9 KB	0 /s	0 /s
docker-service-order-2017.10	● Green	37.5m	20.8 GB	0 /s	0 /s
blazeds	● Green	0	1.9 KB	0 /s	0 /s

Nodes 5 of 5

Name	Status	CPU Usage	Load Average	JVM Memory	Disk Free Space	Shards
elastic-101 172.31.1.101:9300	● Online	1.33 % ↓ 3.33 % max 0 % min	2.24 ↓ 2.46 max 1.17 min	48 % ↑ 51 % max 35 % min	1.0 TB ↑ 1.0 TB max 1.0 TB min	315
elastic-102 172.31.1.102:9300	● Online	1.67 % ↑ 3.33 % max 0.67 % min	1.51 ↑ 2.16 max 1.09 min	50 % ↑ 50 % max 41 % min	1.0 TB ↑ 1.0 TB max 1.0 TB min	315
elastic-103 172.31.1.103:9300	● Online	1.33 % ↑ 2.33 % max 0 % min	1.52 ↓ 2.59 max 1.07 min	51 % ↓ 77 % max 41 % min	1.1 TB ↑ 1.1 TB max 1.1 TB min	314
elastic-78 172.31.1.78:9300	● Online	0 % ↓ 21 % max 0 % min	2.56 ↑ 4.08 max 0.49 min	67 % ↑ 77 % max 64 % min	119.9 GB ↑ 120.1 GB max 119.5 GB min	315
elastic-79 172.31.1.79:9300	● Online	0 % ↑ 6 % max 0 % min	1.11 ↑ 3.65 max 0.28 min	44 % ↑ 66 % max 42 % min	283.8 GB ↓ 283.9 GB max 283.8 GB min	314

技术方案

数据源

Filebeat

Ryslog

Packetbeat

Logstash日志分析

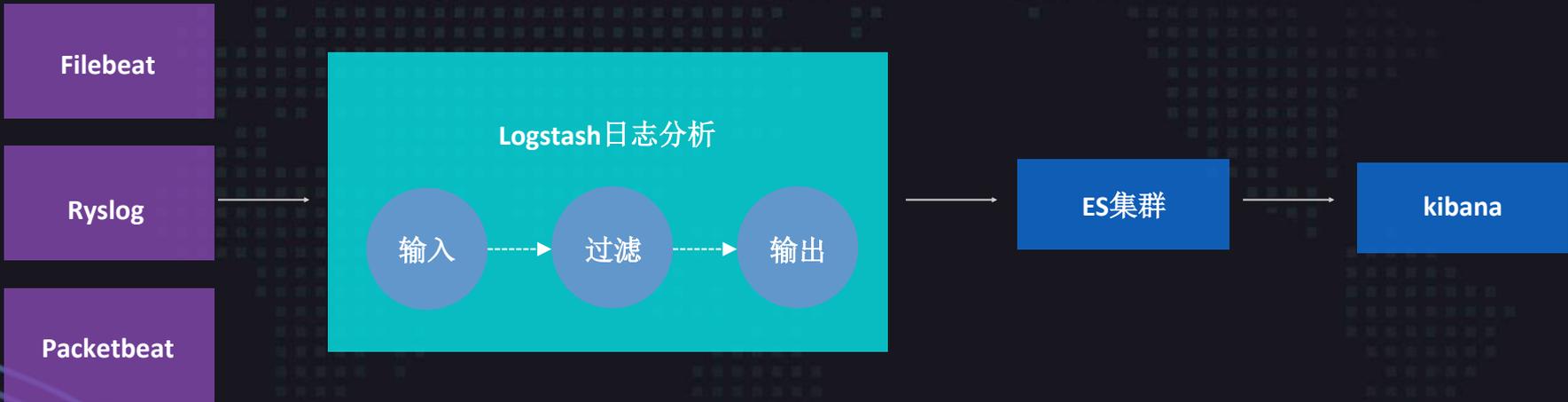
输入

过滤

输出

ES集群

kibana



关键配置

```

input {
  file {
    path => ["/var/lib/docker/containers/*/*-json.log"]
    sinedb_path => "/root/.docker_logstash_sinedb"
    start_position => "beginning"
  }
}
filter {
  json{
    source => message
    add_field => { "service_name" => "%{[attrs][image]}" }
    remove_field => ["attrs"]
  }
  grok {
    match => ["log", "\[(?<log_time>.*?)\]\s(?<log_level>.*?)\b\s(?<content>.*)"]
    match => ["path", "/(?<container_id>\w+)-json.log"]
    remove_field => ["path"]
    remove_field => ["log_time"]
  }
  mutate {
    remove_field => ["log"]
    rename => { "content" => "message" }
    add_field => { "app_env" => "prod" }
  }
}
output {
  if [service_name] != "%{[attrs][image]}"{
    elasticsearch {
      hosts => ["192.168.9.101:9200", "192.168.9.102:9200", "192.168.9.103:9200"]
      index => "docker-%{[service_name]}-%{+YYYY.MM}"
      workers => 20
      template_overwrite => true
    }
  }
}

```

```

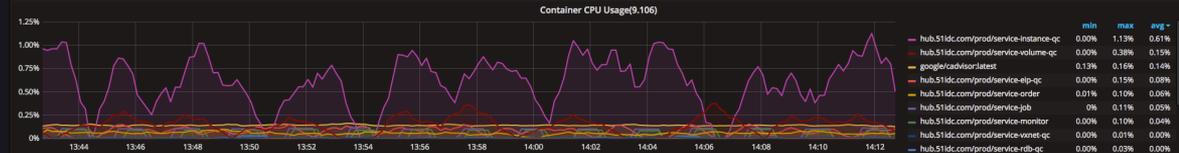
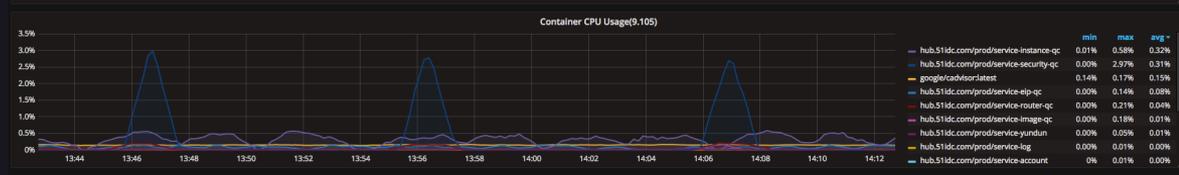
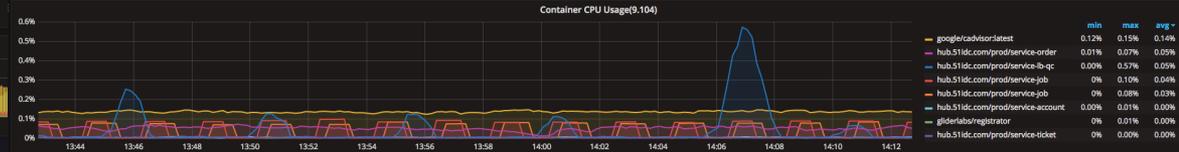
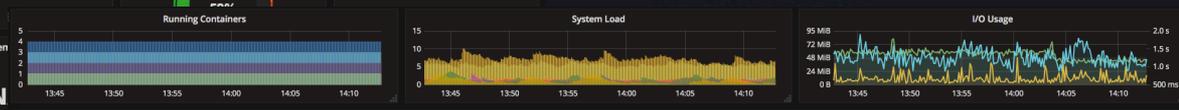
filter {
  grok {
    match => {"message" => "%{IPORHOST:remote_ip} - %{DATA:user_name} \
[%{HTTPDATE:time}]" "%{WORD:request_action} %{DATA:request} HTTP/%{NUMBER:h
ttp_version}" "%{NUMBER:response} %{NUMBER:bytes} "%{DATA:referrer}" "%{DATA
:agent}"}"}
  }
  date {
    match => ["time", "dd/MMM/yyyy:HH:mm:ss Z"]
    target => "time"
  }
  geoiip {
    source => "remote_ip"
    target => "geoiip"
    database => "/opt/logstash-5.1.2/config/GeoLite2-City.mmdb"
  }
  useragent {
    source => "agent"
    target => "user_agent"
  }
  mutate {
    convert => { "bytes" => "integer" }
  }
}
output {
  elasticsearch {
    hosts => ["192.168.9.101:9200", "192.168.9.102:9200", "192.168.9.103:
9200", "192.168.9.78:9200", "192.168.9.79:9200"]
    index => "nginx-log"
    document_type => "log"
    workers => 5
    template => "/etc/logstash/nginx_template.json"
    template_name => "nginx-access"
    template_overwrite => true
  }
}

```

为什么用ELK做监控

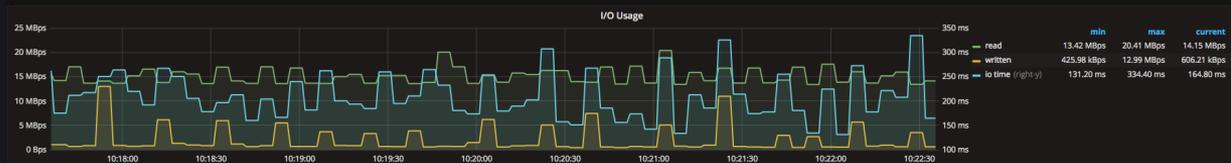
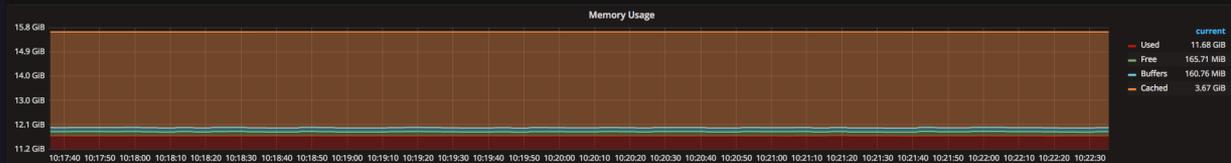
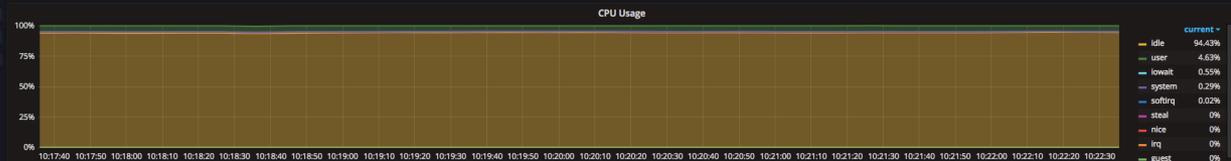
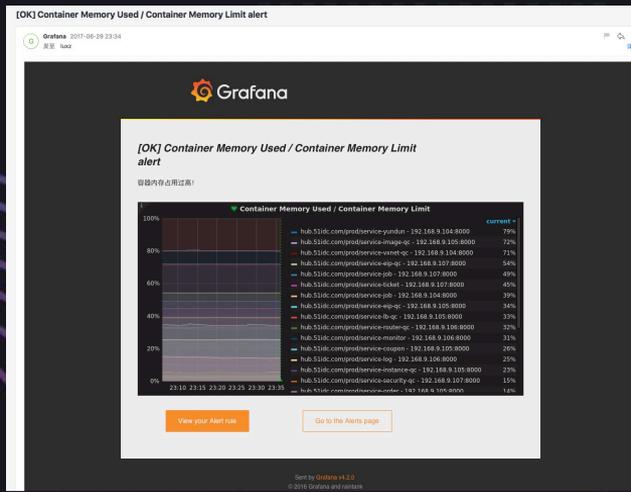
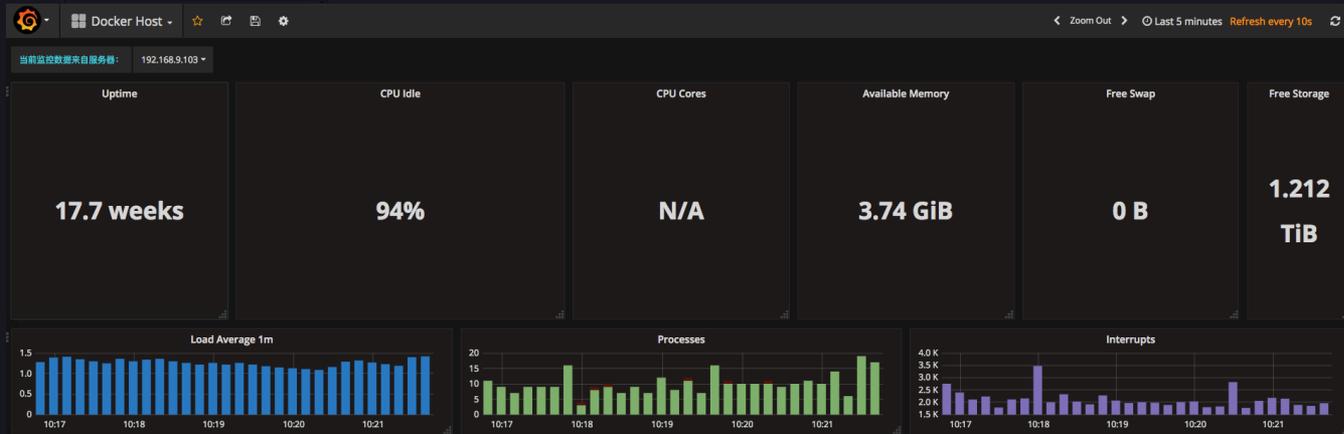
- 节约资源，监控、日志在一个平台搞定
- 降低学习成本，无需额外的学习另外的监控平台
- ELK社区比较活跃，看好ELK的前景
-

Docker 容器监控 Dashboard



主机监控Dashboard

阿里云 MVP



性能指标采集工具

➤ Topbeat

➤ Metricbeat

➤ Collectd

➤ statsd

➤

技术方案

数据源

Metricbeat

topbeat

Packetbeat

Logstash日志分析

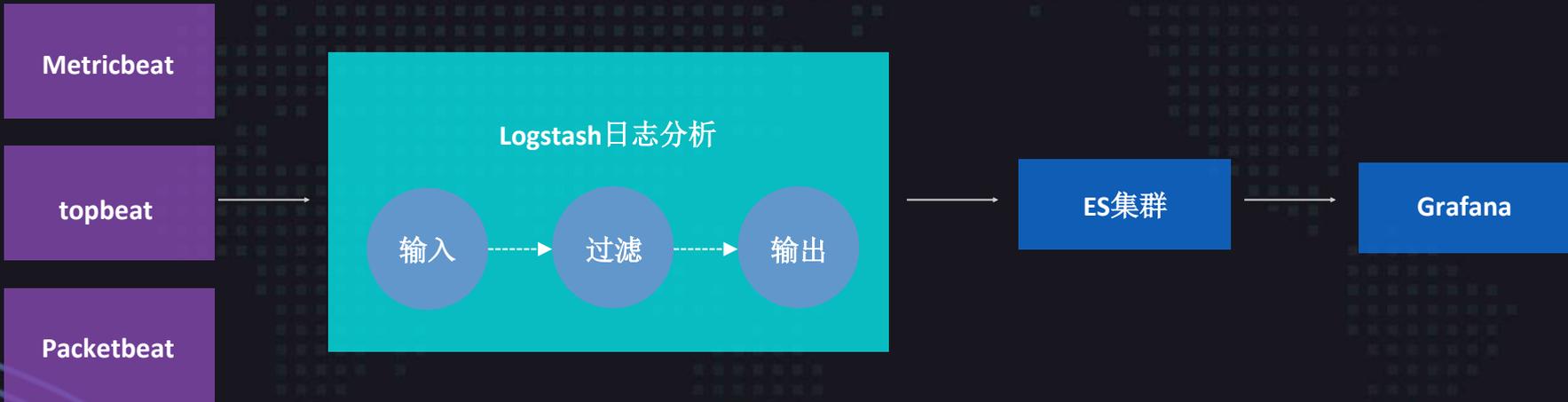
输入

过滤

输出

ES集群

Grafana



ELK优势

- 开源、免费、上手容易
- 实时全文搜索
- 横向可扩展性
- 强大的灵活性
- 。 。 。

ELK使用过程中遇到的问题

- 开源套件没有权限管理
- ES集群的监控告警
- 数据传输没有加密
- 日志审核
- 版本升级



Thanks!