基于elastalert的日志监控实现

目录

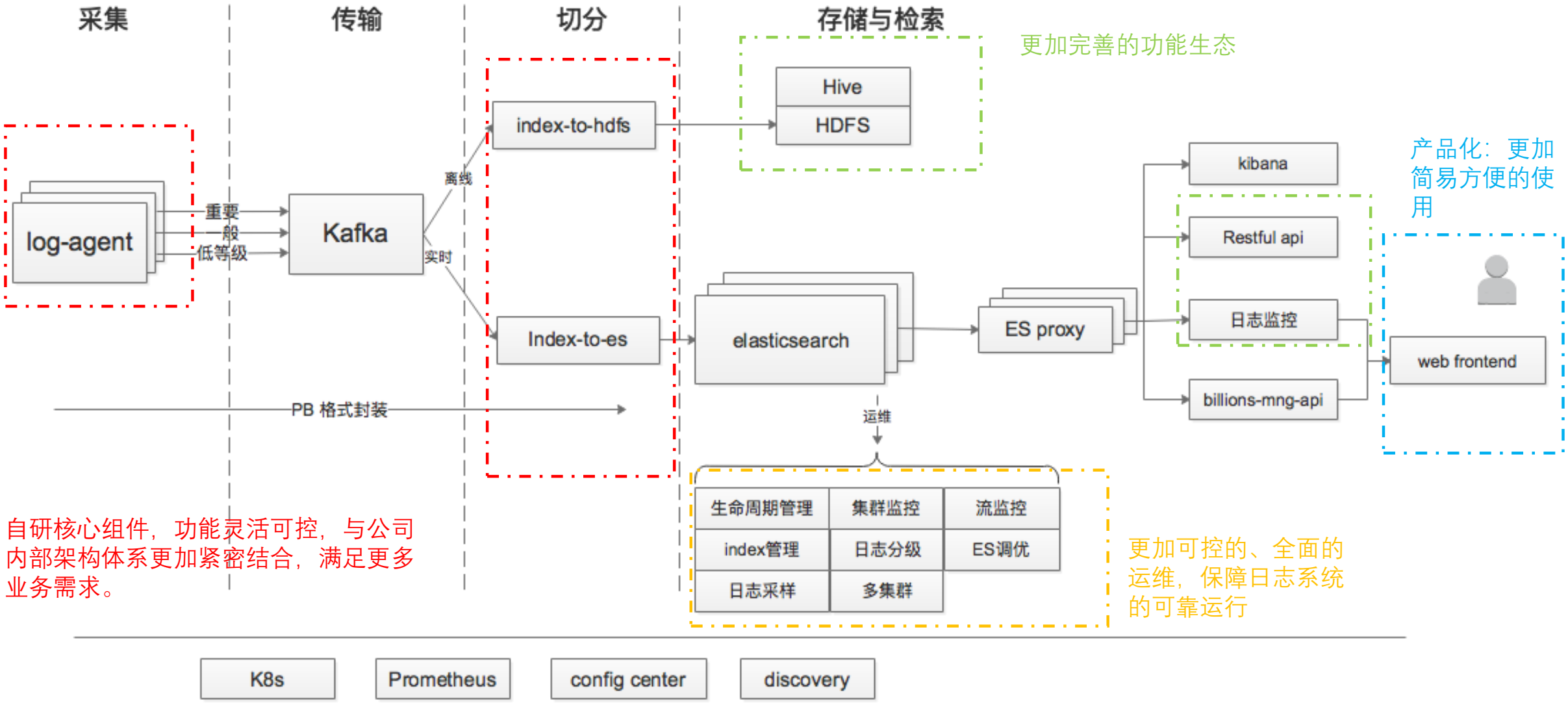
- 日志系统实现简介
- 日志监控的实现：Elastalert的深度第二开发

日志格式规范

- 半结构化JSON作为日志的输出格式
- 包含四类元信息：
  - time: 日志产生时间，ISO8601格式
  - level：日志等级， FATAL、ERROR、WARN、INFO、DEBUG
  - app_id：应用id，用于标示日志来源，与服务树一致，部门.项目.应用 三级，全局唯一
  - instance_id：实例id，用于区分同一应用不同实例，业务方自行设定


```
{
  "time": "2018-06-18T03:00:00.002Z",
  "app_id": "main.community.dm2",
  "instance_id": "dm2-5175-698475c848-qp5gq",
  "level": "INFO",
  "log": " request /x/web-feed/feed/unread succeed",
  "thread_name": "pool-1-thread-245",
  "req": {
    "bucket": "upgcxcode",
    "mission_id": "150e5feb66a6242554d4d8248481b35c",
    "msg": "celery:root_callback:called",
    "request_id": "c9d9992f-527a-4e79-b176-0763d4408c8d",
    "sid": "50001",
  }
}
```

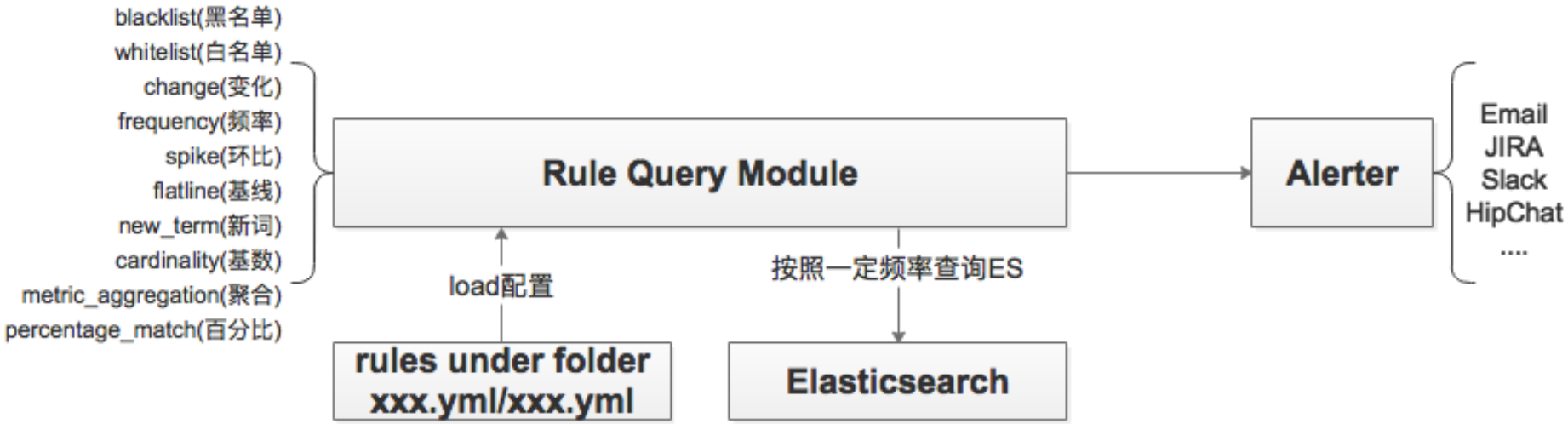
日志系统架构图



自研核心组件，功能灵活可控，与公司内部架构体系更加紧密结合，满足更多业务需求。

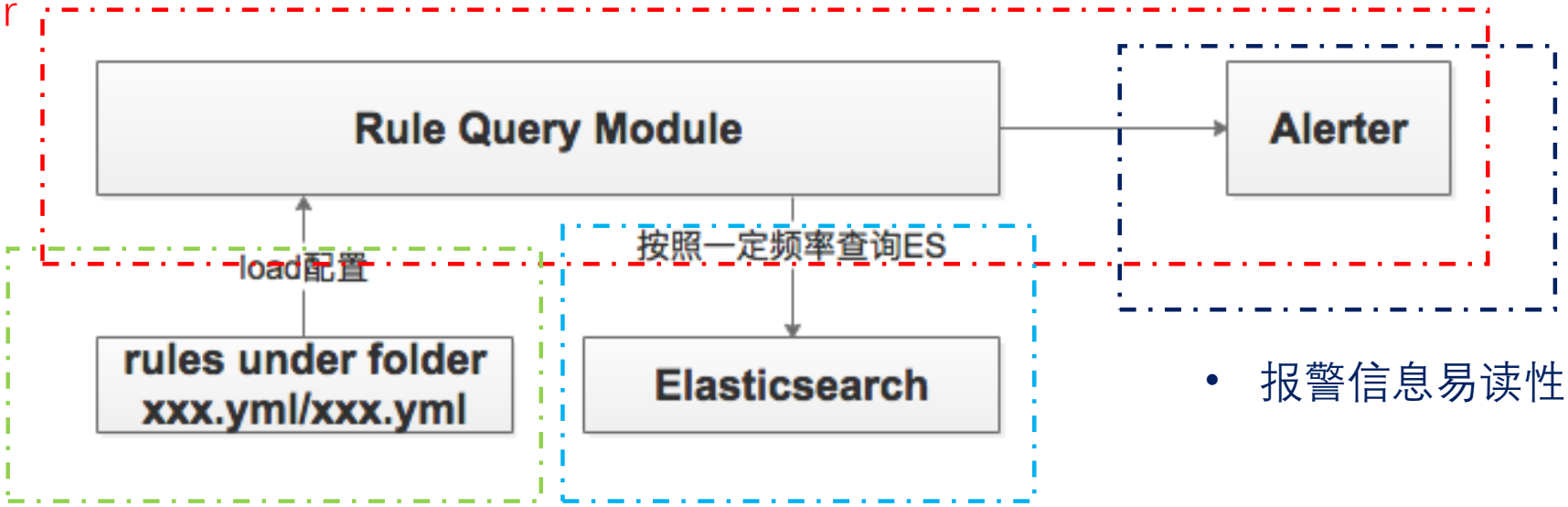
elastalert@Yelp

- Elastalert是Yelp公司用python2写的一个日志报警框架
- https://github.com/Yelp/elastalert
  - 成熟，Github上已有5k+ star
  - 开源，文档全面，方便灵活二次开发
  - 丰富的告警规则和报警方式
  - 代码模块化结构，方便扩展



Elastalert的不足

单实例架构，不支持水平扩展，无法failover



- 报警信息易读性不好

- 基于本地yml方式配置规则，维护成本高
- 配置项目复杂，用户使用门槛高

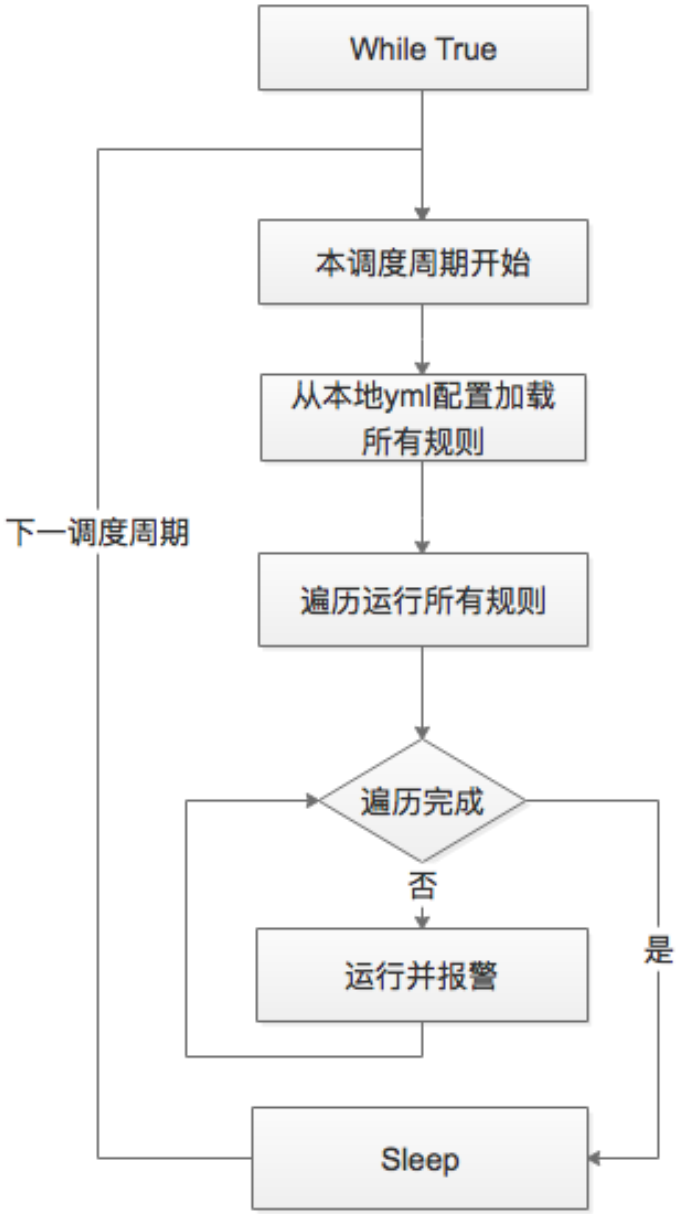
- 查询引擎逻辑复杂，效率一般

Elastalert深度二次开发

- 分布式架构改造
- 核心运行引擎调优
- 产品化提升

分布式架构改造

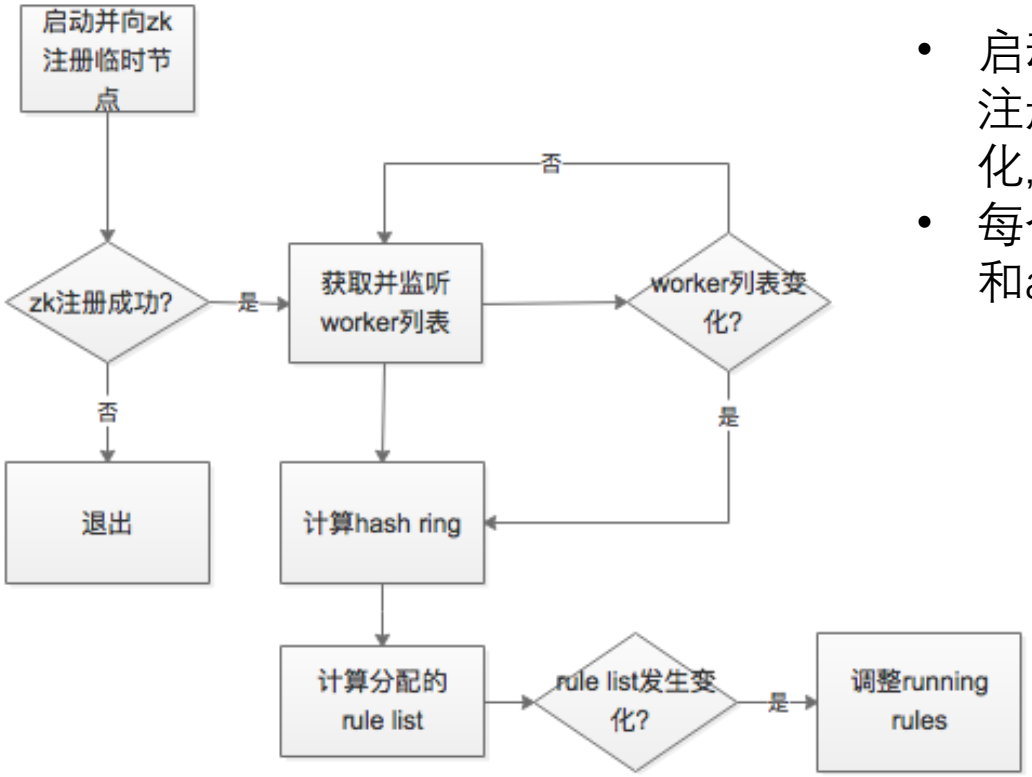
原生规则运行流程图



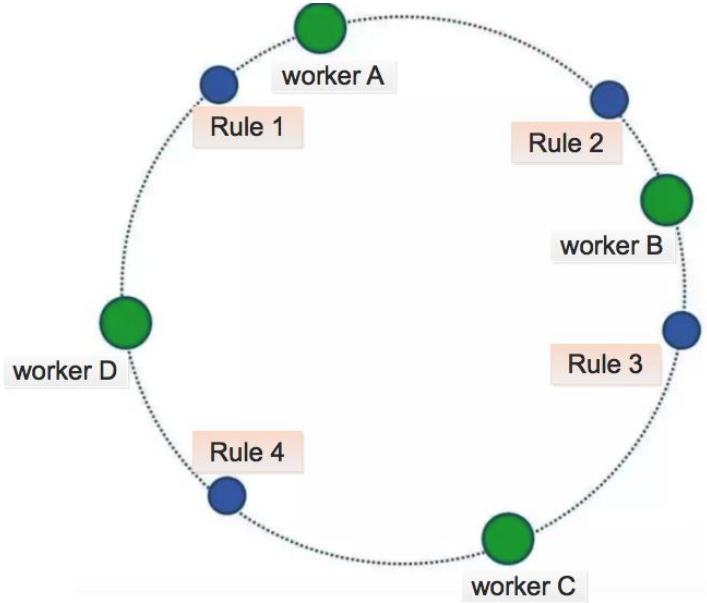
- 配置集中式存储
- workers动态水平扩展
- rules在worker间均匀分配，元信息强一致

分布式架构改造

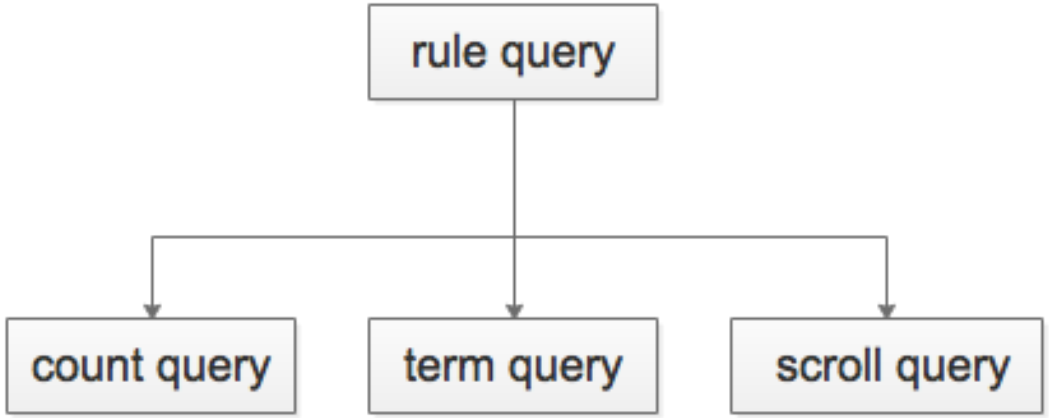
规则集中存储在ES中 + ZooKeeper + 一致性Hash

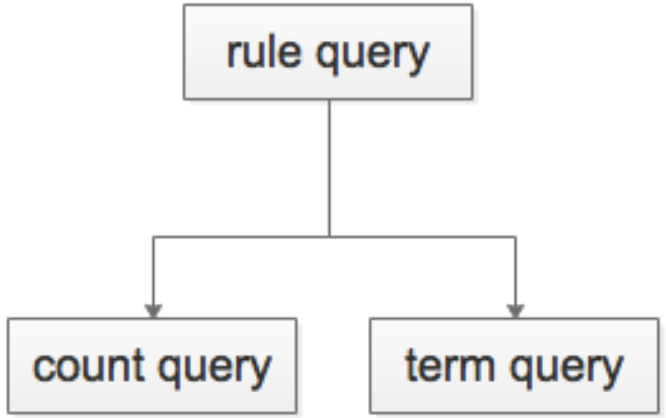


- 启动时以临时节点方式向zk注册，并监控worker list的变化，最终一致性
- 每个运行周期根据worker_list和all_rules重新计算rule list。



核心运行引擎调优





返回匹配数量
优点:
- 执行效率高

缺点:
- 不支持日志详情

根据term进行聚合
优点:
- 执行效率高

缺点:
- 不支持日志详情

根据term进行聚合
优点:
- 支持日志详情

缺点:
- 拉取原始日志到内存中，执行效率低下，内存占用高

- 全部转化为count query或者term query
- 如果需要日志详情，在报警发送之前，做一次size=1的query，附加到报警信息中。
- 最大化执行效率

核心运行引擎简化

```
[(time, count), (time, count), ...]
```

Event Window

- 窗口的长度为rule的时间区间长度：timeframe
- window中的event按照时间排序
- rule每次查询的时间窗口长度为run_every (1 min)
- 根据时间窗口中的累积数据进行报警判断
- 优点：
  - 每次查询之间时间没有重合，查询效率高
- 缺点：
  - 代码逻辑复杂，可维护性不高

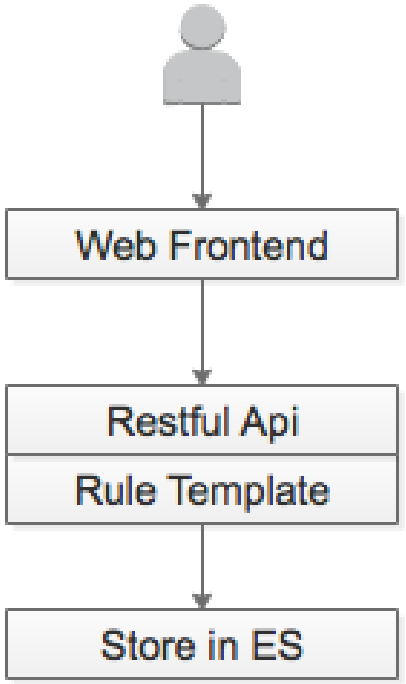
- 每次查询区间为完整的timeframe，摒弃eventwindow
- 性能影响可接受
- 极大简化代码逻辑，便于维护

产品化提升

- 原则：自助操作，简单易用，稳定可靠
- 主要工作：
  - Restful API + web前端
  - 告警优化：格式调整、集成公司内部系统
  - 监控 + Running on K8s

Restful API + web前端

- 日志监控规则使用模板进行封装
  - 只暴露必要配置参数，降低配置复杂度
  - 过滤条件统一通过query_string查询，与kibana一致
- 封装一套Restful Api进行规则的增删改查
- 开发web前端进行报警配置



规则展示

请输入

添加规则 刷 新

状态	启用	告警规则	index	操作	其它
		【Bplus 接入层】用户配置(link_setting)其它接口错误比例告警	billions-bplus-rpc-bplus-gw-@*	修改 删除	日志详情 告警详情
		[dynamic_repost]删除发布内容	billions-bplus-access-dynamic_repost-@*	修改 删除	日志详情 告警详情
		[B端-fe] studio-ssr 服务端，运行错误告警，每分钟错误日志输出超过10...	billions-main.frontend.jinkela-studio-ssr-@*	修改 删除	日志详情 告警详情
		bcd_zone_counter 三十分钟内没有产生日志	billions-video.videodispatch.bcd_zone_counter-@*	修改 删除	日志详情 告警详情
		【会员购】【android】页面秒开率	billions-open.public-service.monitor-end.banner-@*	修改 删除	日志详情 告警详情
		【音频】【iOS】网络请求成功率	billions-open.public-service.monitor-end.music-@*	修改 删除	日志详情 告警详情
		mall-cron ERROR 报警	billions-mall-cron-@*	修改 删除	日志详情 告警详情
		open.pay.open-pay-merchant ERROR 报警	billions-open.pay.open-pay-merchant-@*	修改 删除	日志详情 告警详情
		pay-apigateway ERROR 报警	billions-openplatform-pay-apigateway-@*	修改 删除	日志详情 告警详情
		活动页面报警（活动页面炸了～～）	billions-main.frontend.bilibili-log-report-seed-@*	修改 删除	日志详情 告警详情

共1005条 < 1 2 3 4 5 6 ··· 101 > 10 条/页

规则添加

添加规则 返回

* 监控类型：频率监控

* index：

* 报警名称：

* 日志过滤规则：填写日志过滤规则，不支持换行

帮助

* 报警策略：1 分钟内 大于等于 阈值

及时告警：

开启：若告警策略时间窗口设置为3分钟，两分钟内若达到阈值即会告警。

关闭：按照设置的时间窗口长度计算阈值。

* realert：1 分钟

相同两条告警发送间隔时间。默认为报警策略时间窗口。

聚合字段：可选

可选，对于指定字段的每个unique value（目前只支持一个字段）分别进行报警计算

开启：

报警配置

* 报警方式：skyeye

通用报警请使用skyeye

* 级别：

帮助

告警屏蔽时间设置：

时间段：请选择时间 至 请选择时间

日期： 至

报警包含日志详情：

对于大日志量的服务请谨慎开启日志详情功能(执行开销较大)

报警接收人：多个用户以逗号分隔

接收人之间用,间隔

报警接收服务树：发送给对应节点的op,rd

发送给对应节点的op,rd

接收人和服务树至少二选一

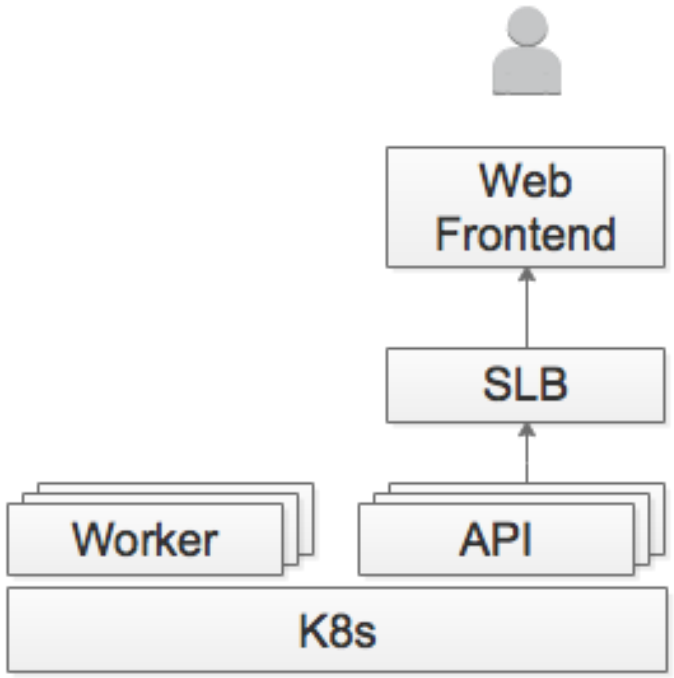
告警优化

- 与公司内告警平台进行集成
- 格式调整（汉化、易读性）
- 功能迭代
  - 报警屏蔽
  - 报警组
  - 报警确认
  - 报警级别设置

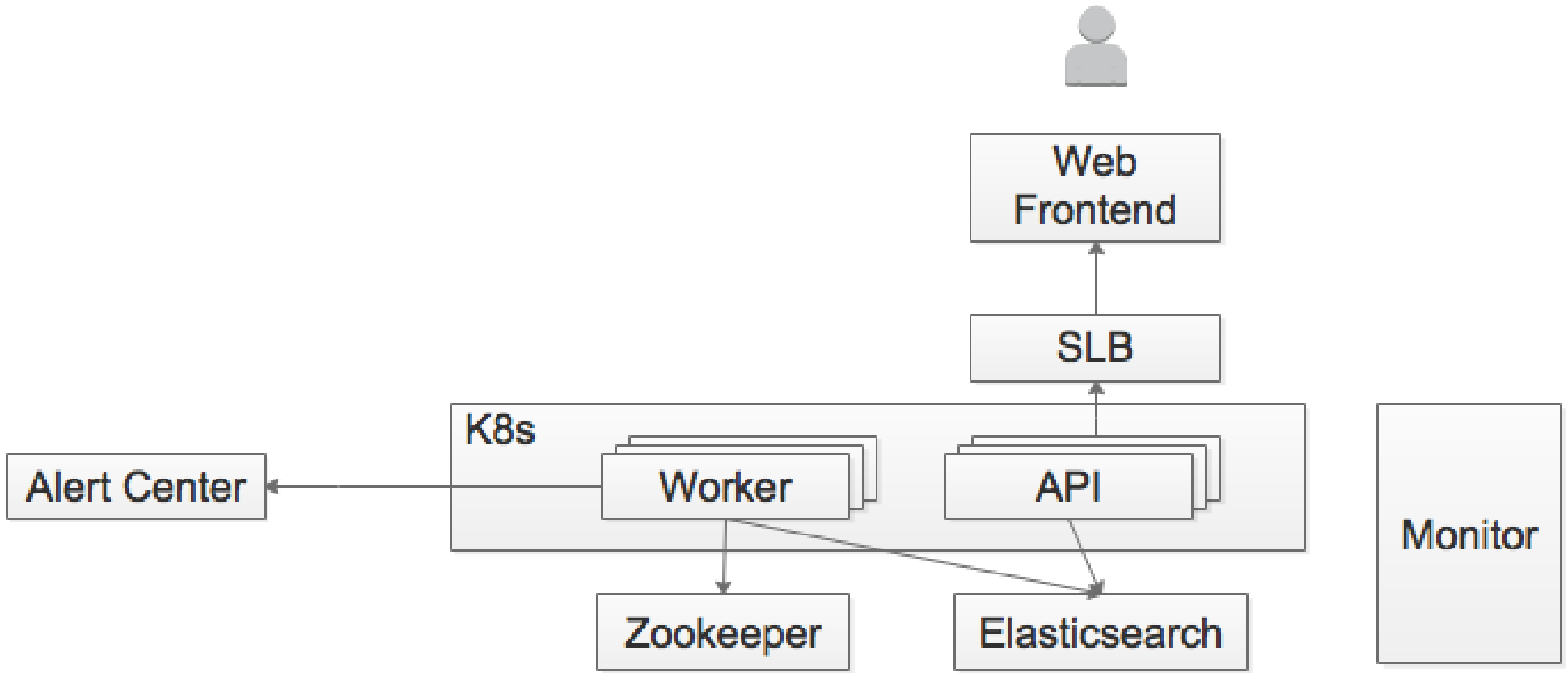
```
日志报警：[Billions] 定时告警-频率监控

发生了600次事件，时间:2019-04-02 07:47 CST至2019-04-02 07:48 CST

详情示例：
app_id: ops.billions.fake_flow.000161
instance_id: fake-app-000161-29838-5999478b7f-f6xsl
level: INFO
log: hello billions, write more
logDelay: 7.891005709
run: 12
special: value
```

稳定可靠的运维

- All on K8s
- 全面的监控
  - 异常错误
  - 执行耗时
  - 报警发送
  - 定时fake监控



整体架构


Web
Frontend
SLB
K8s
Alert Center
Worker
API
Monitor
Zookeeper
Elasticsearch

Thanks

elastic
中文社区

专业、垂直、纯粹的 Elastic 开源技术交流社区

https://elasticsearch.cn/