**APM性能⽇志传输解决⽅案**

1. ⽇志传输解决⽅案设计

2. fifilebeat 采集配置与实现

3. fifilebeat 集成 logstatsh & elasticsearch

**⼀、⽇志传输解决⽅案设计**

⼀个完整的APM系统，包含如下基本模块：

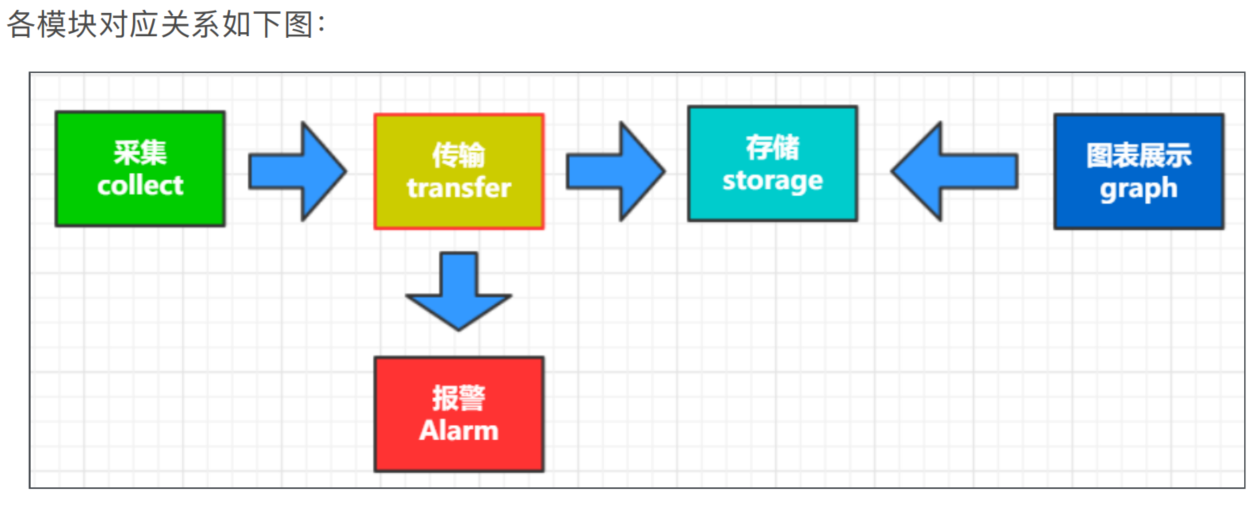
1. 性能⽇志采集

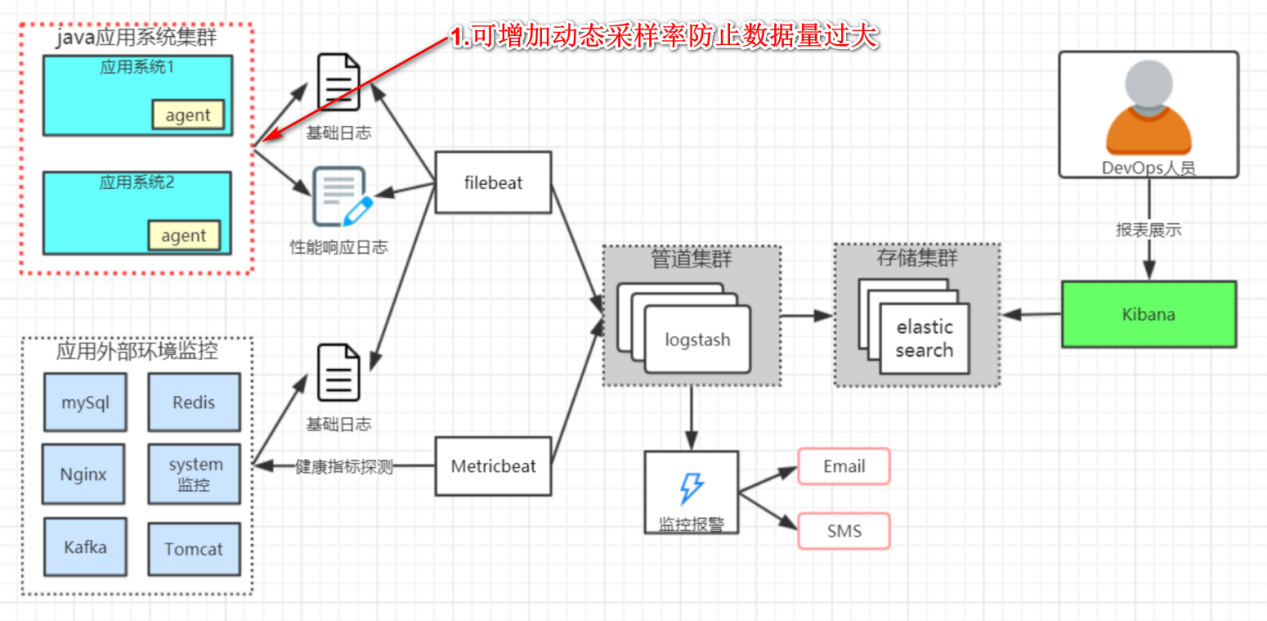
2. 数据传输

3. 异常判定与报警

4. 数据存储

5. 图表展示



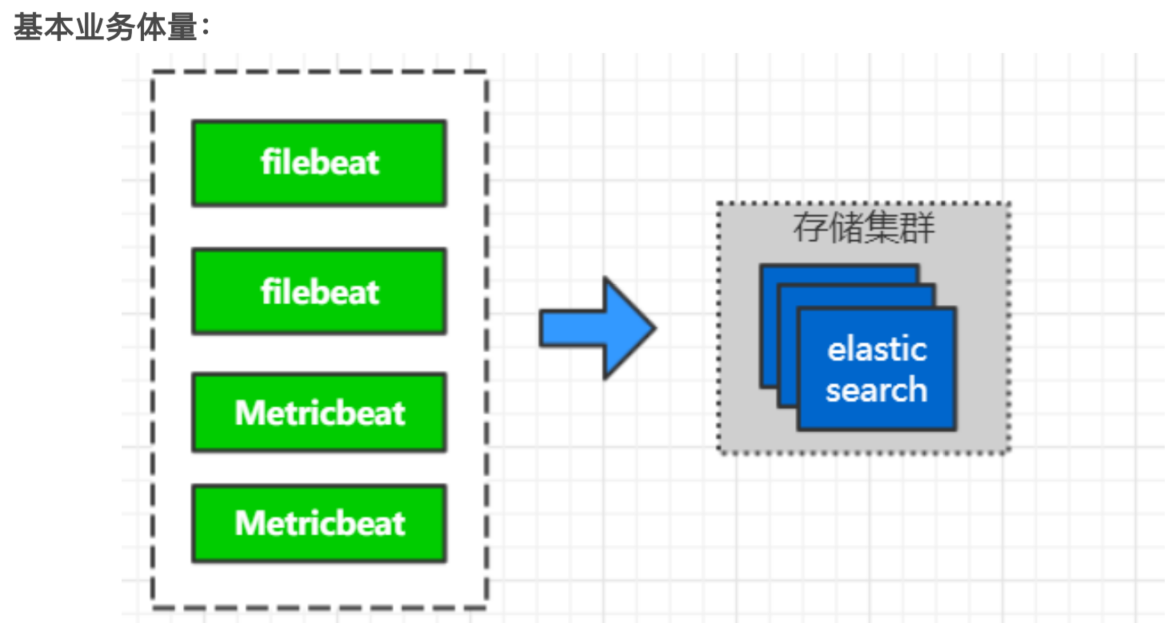


**2、传输模块具体解决⽅案**

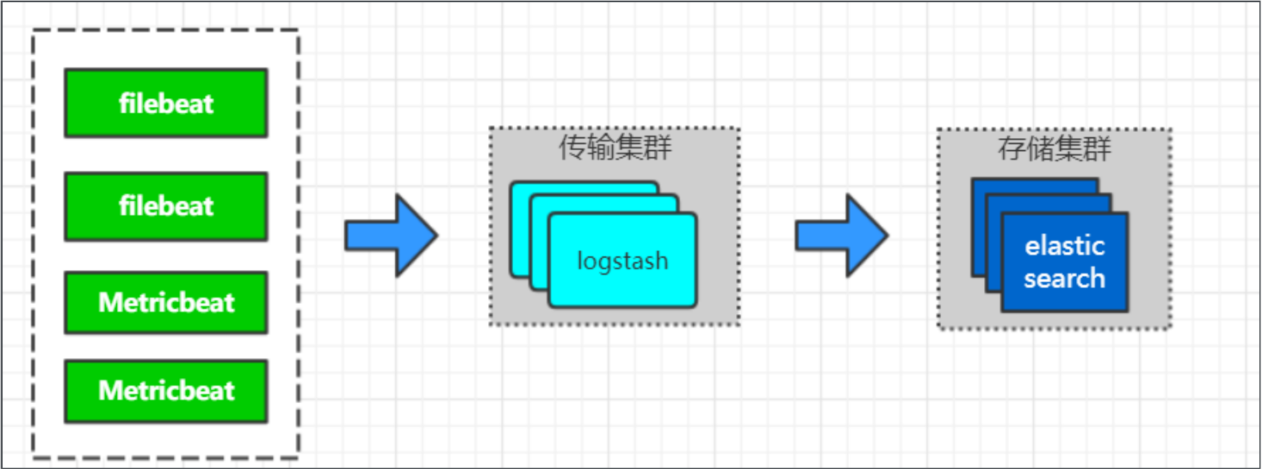
传输模块的设计⽬标在于两点：

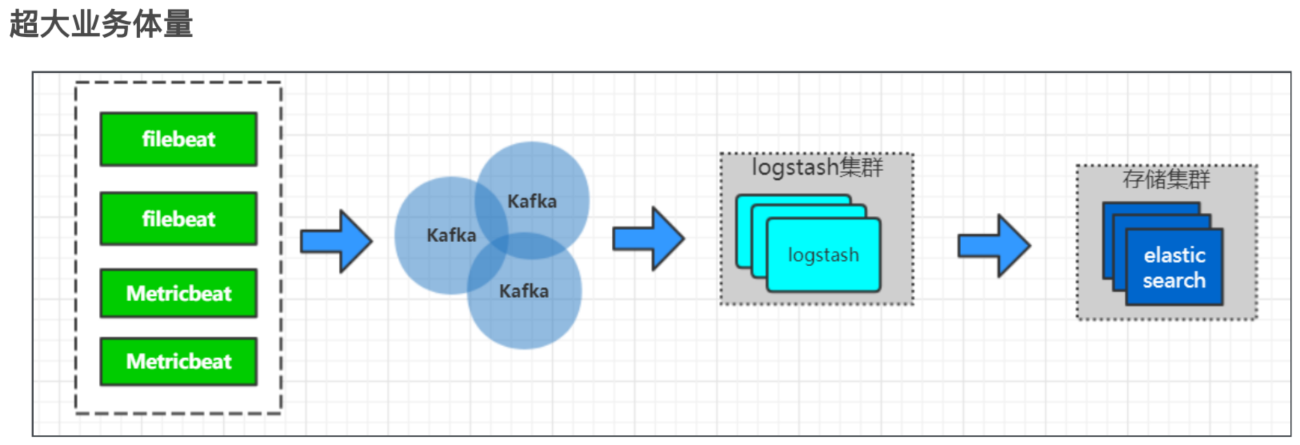
1. 保证信息能够顺利传输⾄报警判定中⼼与存储中⼼。

2. 可基于不同业务体量灵活调整架构规模，控制维护成本。



中等业务体量：





<https://www.elastic.co/cn/products/beats>

Beats 平台集合了多种单一用途数据采集器。它们从成百上千或成千上万台机器和系统向 Logstash 或 Elasticsearch 发送数据。

[Filebeat](https://www.elastic.co/cn/products/beats/filebeat) 和 [Metricbeat](https://www.elastic.co/cn/products/beats/metricbeat) 内部集成了一系列模块，用以简化常见日志格式（例如 NGINX、Apache 或诸如 Redis 或 Docker 等系统指标）的收集、解析和可视化过程。只需运行一行命令，即可开始探索。

<https://www.elastic.co/cn/products/logstash>

Logstash 是开源的服务器端数据处理管道，能够同时从多个来源采集数据，转换数据，然后将数据发送到您最喜欢的“存储库”中。

Logstash 能够动态地采集、转换和传输数据，不受格式或复杂度的影响。利用 Grok 从非结构化数据中派生出结构，从 IP 地址解码出地理坐标，匿名化或排除敏感字段，并简化整体处理过程。

**⼆、fifilebeat 采集配置与实现**

1. fifilebeat 简介

2. fifilebeat 安装与简单使⽤

3. fifilebeat 参数说明

**1、fifilebeat 简介**

fifilebeat 是elastic Beats 平台的⼀员，使⽤GO语⾔开发，期主⽤途为⽂件数据采集器。这些采集器安装后可⽤作轻量型代理，从成百上千或成千上万台机器向 Logstash 或 Elasticsearch 发送数据。其主要特点如下：

1. **轻量**：对使⽤环境⽆依懒。

2. **即插即⽤**：内部集成了⼀系列模块，⽤以简化收集、解析和可视化常⻅⽇志格式，诸如： NGINX、Apache

3. **可扩展** 可基于libbeat 自行构建采集器

**2、fifilebeat 安装 与使⽤**

前往elastic 官⽹下载fifilebeat 指定版本 https://www.elastic.co/downloads/past-releases

#下载

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.6.6-linux-x86\_64.tar.gz

# 解压

tar -zxvf filebeat-5.6.6-linux-x86\_64.tar.gz

#编辑配置文件

vim filebeat.yml

#启动

./filebeat

#后台启动

$nohup ./filebeat &

*注：本次项⽬启⽤的Elastic系统版本统⼀为V5.6.6*

**3、fifilebeat参数说明**

常⽤的fifilebeat 分为三个部分

1. prospectors 采集配置

2. Output 输出配置

3. global与 General 公共配置与⼀般配置

采⽤YAML 语⾔做为其配置语法。它的基本语法规则如下。

1. ⼤⼩写敏感

2. 使⽤缩进表示层级关系

3. 缩进时不允许使⽤Tab键，只允许使⽤空格。

4. 缩进的空格数⽬不重要，只要相同层级的元素左侧对⻬即可

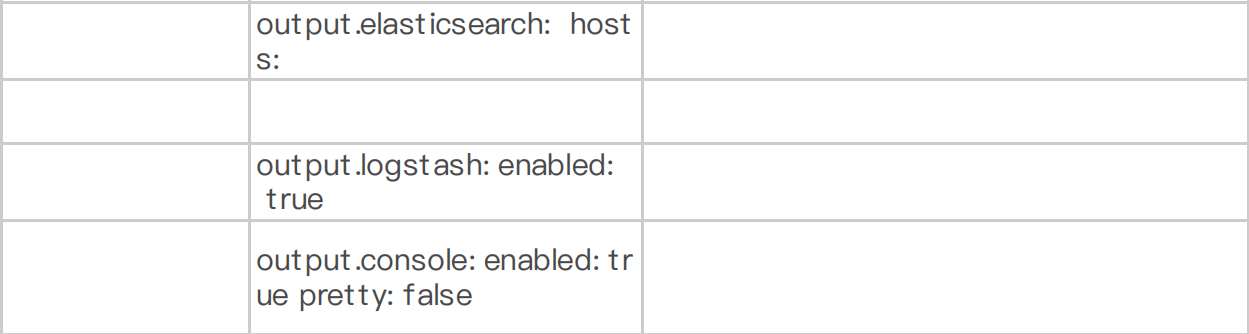


- 表示数组

具体配置说明







**三、fifilebeat集成logstatsh & elasticsearch**

1. logstatsh & elasticsearch &Kibana 安装

2. fifilebeat 集成logstash

3. fifilebeat 集成elasticesarch

1、logstatsh & elasticsearch &Kibana 安装

前往 elastic 下载 3个软件的5.6.6 版本 https://www.elastic.co/downloads/past-releases添另es⽤户（elasticsearch 不允许⽤root启动）

useradd es

2、fifilebeat 集成logstash

**Nginx ⽇志配置**

**FileBeat 配置**

编辑fifilebeat.yml配置⽂件



**logstash 配置**

**编写写** beats.conf

vim conf/beats.conf

在beats.conf 当中添加以下内容



启动：./bin/logstash -f config/beats.conf

1. fifilebeat 集成elasticesarch

**⼀、基于Elasticsearch⽇志存储实践**

概要：

1. Elasticsearch简介

2. mapping 说明

3. APM 数据存储实践

1、Elasticsearch 简介

Elasticsearch 是⼀个分布式的 RESTful ⻛格的搜索和数据分析引擎,底层基于luncene实

现。

**基础概念：**

* 集群(Cluster)
* 节点(Node)
* 索引(Index)
* 类型(Type)
* ⽂档(Document)
* 分⽚和复制(Shards & Replicas)
* 结构化映谢 （mapping）



2、Elasticsearch mapping 配置说明

1. string类型

2. text类型

3. keyword类型

4. 数字类型

5. Object类型

6. date类型

7. Array类型

8. binary类型

9. ip类型

10. range类型

11. nested类型

12. token\_count类型

13. geo point 类型

1. APM 数据存储实践

Filebeat

配置需要扫描哪些log文件

输出到logstash地址

Logstash

配置文件 beats.conf apm.json

运行 ./bin/logstash -f config/beats.conf

Kibana es 修改一下host配置 直接运行即可