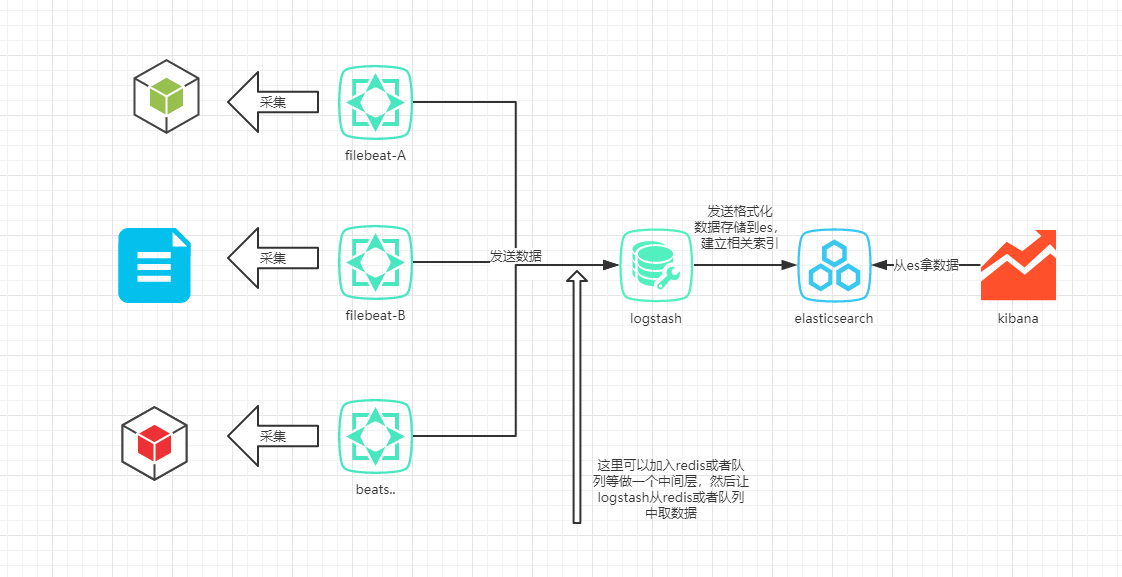
ELK日志收集系统方案架构： （此图来源于网友）



# 官方下载docker镜像

# <https://www.docker.elastic.co/#>

# 注 4个组件版本尽量一致 本次全部采用 6.4.2 版本

# 运行es

docker run -d --restart=always -p 9200:9200 -p 9300:9300 --name elasticsearch -e "discovery.type=single-node" docker.elastic.co/elasticsearch/elasticsearch:6.4.2

# 运行kibana

docker run -d --restart=always --name kibana -p 5601:5601 --link elasticsearch -e ELASTICSEARCH\_URL=http://elasticsearch:9200 docker.elastic.co/kibana/kibana:6.4.2

# 编写logstash.conf文件

input {

beats {

#host => "localhost"

port => "5043"

}

}

filter {

if [fields][doc\_type] == 'test' {

grok {

match => { "message" => "%{TIMESTAMP\_ISO8601:timestamp} %{LOGLEVEL:level} %{JAVALOGMESSAGE:msg}" }

}

}

}

output {

stdout { codec => rubydebug }

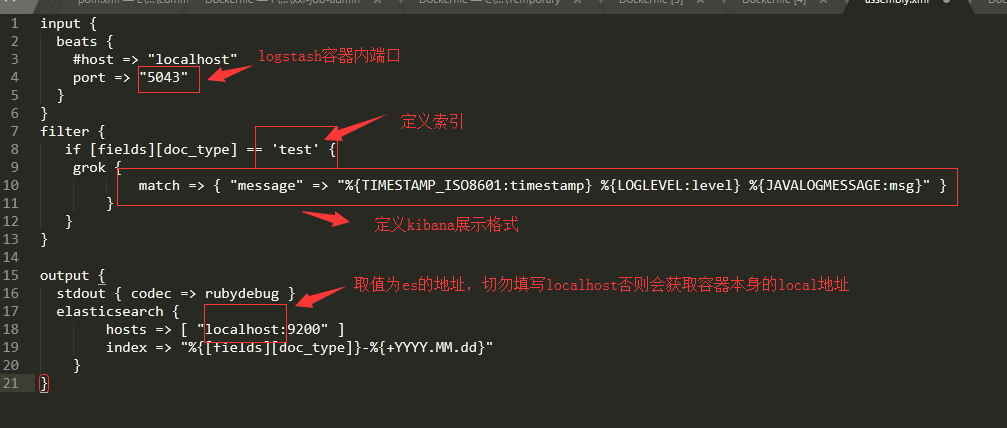
elasticsearch {

hosts => [ "elasticsearch:9200" ]

index => "%{[fields][doc\_type]}-%{+YYYY.MM.dd}"

}

}



# 编写 filebeat.yml 文件

filebeat.prospectors:

- paths:

- /home/logs/\*.log

multiline:

pattern: ^\d{4}

negate: true

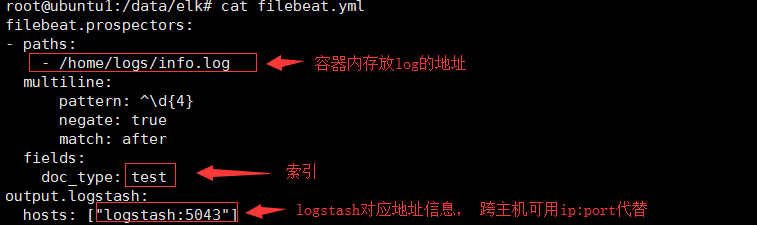
match: after

fields:

doc\_type: test

output.logstash:

hosts: ["logstash:5043"]



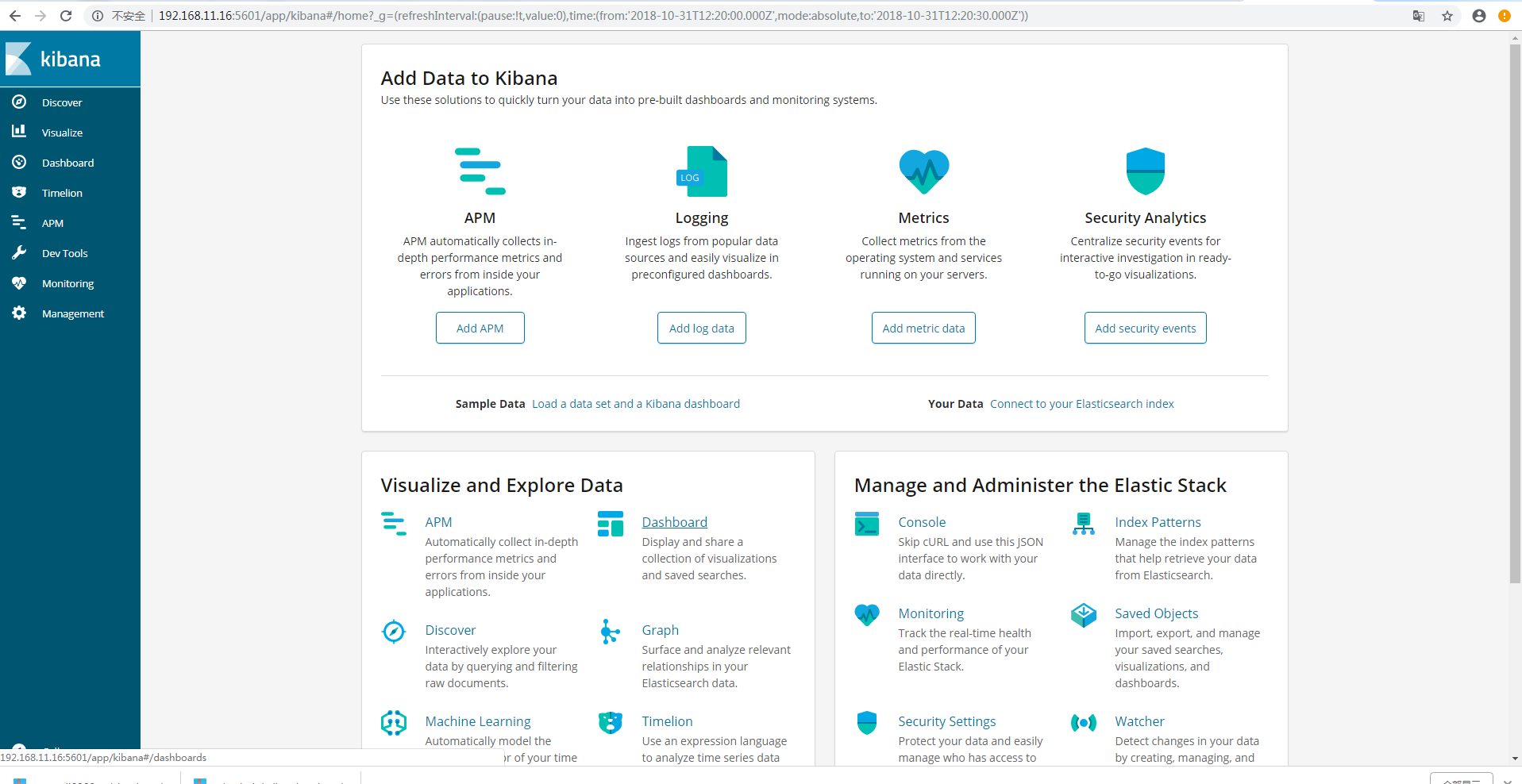
# 运行logstash -v 左侧为宿主机目录 右侧为容器配置文件地址

docker run -it --restart=always --name logstash --link elasticsearch -d -v /data/elk/logstash.conf:/usr/share/logstash/pipeline/logstash.conf docker.elastic.co/logstash/logstash:6.4.2

# 运行 filebeat

docker run --restart=always --name filebeat -d --link logstash -v /data/elk/filebeat.yml:/usr/share/filebeat/filebeat.yml -v /var/www/html/ifaas/api/logs/:/home/logs/ docker.elastic.co/beats/filebeat:6.4.2

# 浏览器打开



# 点击 index patterns

