filebeat安装收集日志

1.安装

> 安装方式：yum

```
# 安装 GPG-KEY
rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

# 设置filebeat的yum源文件
vi /etc/yum.repos.d/beat.repo
# 将以下内容粘贴入beat.repo中
[beats]
name=Elastic Beats Repository
baseurl=https://packages.elastic.co/beats/yum/el/$basearch
enabled=1
gpgkey=https://packages.elastic.co/GPG-KEY-elasticsearch
gpgcheck=1

# 开始安装
yum -y install filebeat

# 设置开机启动
chkconfig filebeat on 或者 chkconfig --add filebeat

# 启动
service filebeat start
```

2.配置文件

> 配置文件目录: /etc/filebeat/filebeat.yml

```
filebeat:
  prospectors:
    -
      paths:
        - /var/logs/*.log   # 日志路径
      multiline:    # 匹配日志信息规则
          pattern: '^[[:space:]]'  # 遵循golang的正则语法
          negate: true
          match: after

# 输出日志到elasticsearch服务器上
output:
  elasticsearch:
    hosts: ["192.168.1.118:9200"]

# 指定标签,利于后续在kibana中筛选数据
shipper:
  tags: ["web"]
```