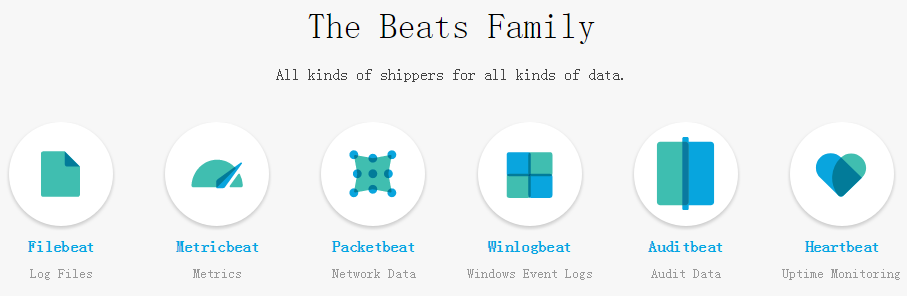
# **[开始使用Filebeat](https://www.cnblogs.com/cjsblog/p/9445792.html)**

## **认识Beats**

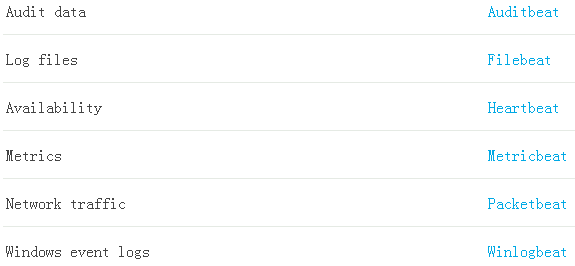


Beats是用于单用途数据托运人的平台。它们以轻量级代理的形式安装，并将来自成百上千台机器的数据发送到Logstash或Elasticsearch。

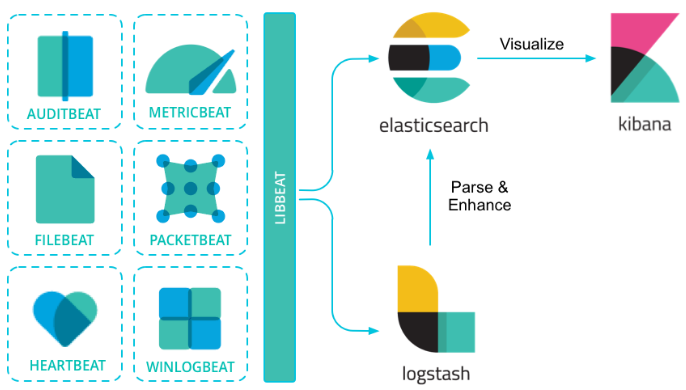
（画外音：通俗地理解，就是**采集数据**，并**上报**到Logstash或Elasticsearch）

Beats对于收集数据非常有用。它们位于你的服务器上，将数据集中在Elasticsearch中，Beats也可以发送到Logstash来进行转换和解析。

为了捕捉（捕获）数据，Elastic提供了各种Beats：

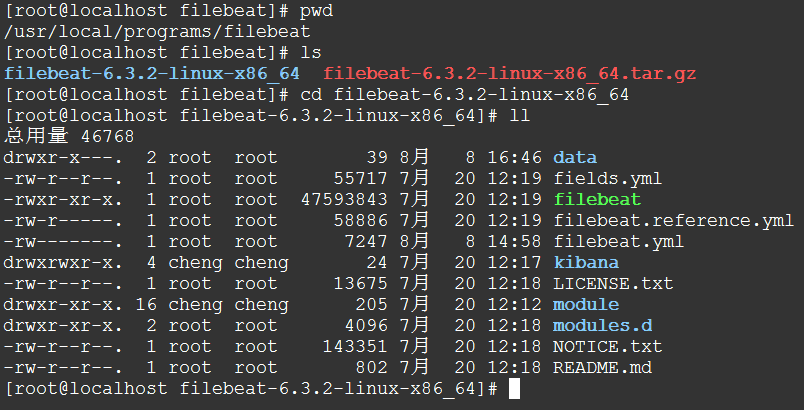


Beats可以直接（或者通过Logstash）将数据发送到Elasticsearch，在那里你可以进一步处理和增强数据，然后在Kibana中将其可视化。



## **Filebeat**

### **第1步：安装Filebeat**



### **第2步：配置Filebeat**

配置文件：filebeat.yml

为了配置Filebeat：

**1. 定义日志文件路径**

对于最基本的Filebeat配置，你可以使用单个路径。例如：

filebeat.inputs:- type: log

enabled: true

paths:

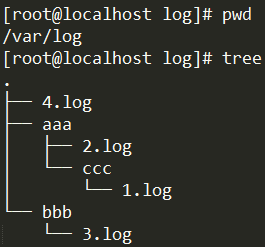
- /var/log/\*.log

在这个例子中，获取在/var/log/\*.log路径下的所有文件作为输入，这就意味着Filebeat将获取/var/log目录下所有以.log结尾的文件。

为了从预定义的子目录级别下抓取所有文件，可以使用以下模式：/var/log/\*/\*.log。这将抓取/var/log的子文件夹下所有的以.log结尾的文件。它不会从/var/log文件夹本身抓取。目前，不可能递归地抓取这个目录下的所有子目录下的所有.log文件。

（画外音：

　　假设配置的输入路径是/var/log/\*/\*.log，假设目录结构是这样的：



　　那么只会抓取到2.log和3.log，而不会抓到1.log和4.log。因为/var/log/aaa/ccc/1.log和/var/log/4.log不会被抓到。

）

**2. 如果你发送输出目录到Elasticsearch（并且不用Logstash），那么设置IP地址和端口以便能够找到Elasticsearch：**

output.elasticsearch:

hosts: ["192.168.1.42:9200"]

**3. 如果你打算用Kibana仪表盘，可以这样配置Kibana端点：**

setup.kibana:

host: "localhost:5601"

**4. 如果你的Elasticsearch和Kibana配置了安全策略，那么在你启动Filebeat之前需要在配置文件中指定访问凭据。例如：**

[IMG_261](https://www.cnblogs.com/cjsblog/p/javascript:void(0);)

output.elasticsearch:

hosts: ["myEShost:9200"]

username: "filebeat\_internal"

password: "{pwd}"

setup.kibana:

host: "mykibanahost:5601"

username: "my\_kibana\_user"

password: "{pwd}"

[IMG_262](https://www.cnblogs.com/cjsblog/p/javascript:void(0);)

### **第3步：配置Filebeat以使用Logstash**

如果你想使用Logstash对Filebeat收集的数据执行额外的处理，那么你需要将Filebeat配置为使用Logstash。

output.logstash:

hosts: ["127.0.0.1:5044"]

### **第4步：在Elasticsearch中加载索引模板**

在Elasticsearch中，索引模板用于定义设置和映射，以确定如何分析字段。（画外音：相当于定义索引文档的数据结构，因为要把采集的数据转成标准格式输出）

Filebeat包已经安装了推荐的索引模板。如果你接受filebeat.yml中的默认配置，那么Filebeat在成功连接到Elasticsearch以后会自动加载模板。如果模板已经存在，不会覆盖，除非你配置了必须这样做。

通过在Filebeat配置文件中配置模板加载选项，你可以禁用自动模板加载，或者自动加载你自己的目标。

**配置模板加载**

默认情况下，如果Elasticsearch输出是启用的，那么Filebeat会自动加载推荐的模板文件 ——— fields.yml。

* 加载不同的模板

setup.template.name: "your\_template\_name"

setup.template.fields: "path/to/fields.yml"

覆盖一个已存在的模板

setup.template.overwrite: true

禁用自动加载模板

setup.template.enabled: false

修改索引名称

# 默认情况下，Filebeat写事件到名为filebeat-6.3.2-yyyy.MM.dd的索引，其中yyyy.MM.dd是事件被索引的日期。为了用一个不同的名字，你可以在Elasticsearch输出中设置index选项。例如：

output.elasticsearch.index: "customname-%{[beat.version]}-%{+yyyy.MM.dd}"

setup.template.name: "customname"

setup.template.pattern: "customname-\*"

setup.dashboards.index: "customname-\*"

**手动加载模板**

./filebeat setup --template -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'

### **第5步：设置Kibana dashboards**

Filebeat附带了Kibana仪表盘、可视化示例。在你用dashboards之前，你需要创建索引模式，filebeat-\*，并且加载dashboards到Kibana中。为此，你可以运行setup命令或者在filebeat.yml配置文件中配置dashboard加载。

./filebeat setup --dashboards

### **第6步：启动Filebeat**

./filebeat -e -c filebeat.yml -d "publish"

### **第7步：查看Kibana仪表板示例**

http://127.0.0.1:5601

## **完整的配置**

[IMG_263](https://www.cnblogs.com/cjsblog/p/javascript:void(0);)

#=========================== Filebeat inputs ==============

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/\*.log

#============================== Dashboards ===============

setup.dashboards.enabled: false

#============================== Kibana ==================

setup.kibana:

host: "192.168.101.5:5601"

#-------------------------- Elasticsearch output ---------

output.elasticsearch:

hosts: ["localhost:9200"]

[IMG_264](https://www.cnblogs.com/cjsblog/p/javascript:void(0);)

**启动Elasticsearch**

　　/usr/local/programs/elasticsearch/elasticsearch-6.3.2/bin/elasticsearch

**启动Kibana**

　　/usr/local/programs/kibana/kibana-6.3.2-linux-x86\_64/bin/kibana

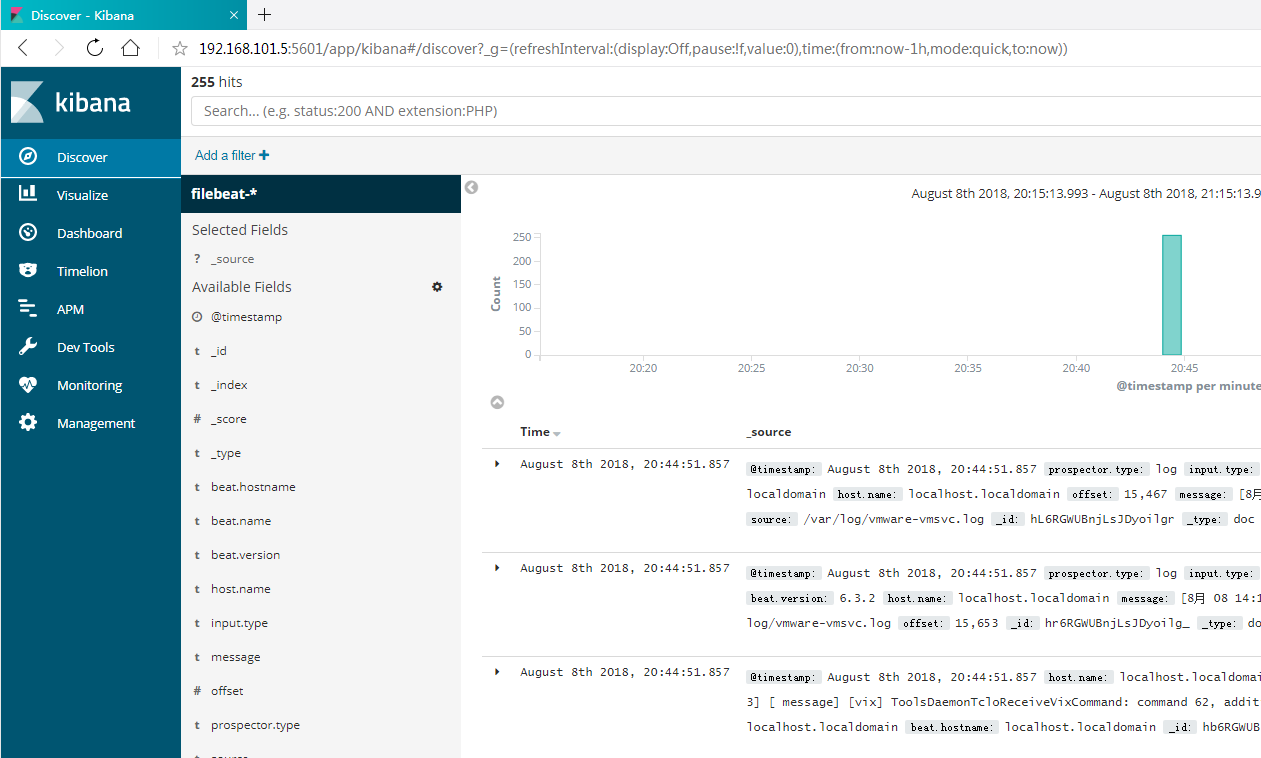
**设置dashboard**

　　./filebeat setup --dashboards

**启动Filebeat**

　　./filebeat -e -c filebeat.yml -d "publish"

**浏览器访问  http://192.168.101.5:5601**



**查看索引**

请求：

curl -X GET "localhost:9200/\_cat/indices?v"

响应：

health status index uuid pri rep docs.count docs.deleted store.size pri.store.size

yellow open bank 59jD3B4FR8iifWWjrdMzUg 5 1 1000 0 475.1kb 475.1kb

green open .kibana DzGTSDo9SHSHcNH6rxYHHA 1 0 153 23 216.8kb 216.8kb

yellow open filebeat-6.3.2-2018.08.08 otgYPvsgR3Ot-2GDcw\_Upg 3 1 255 0 63.7kb 63.7kb

yellow open customer DoM-O7QmRk-6f3Iuls7X6Q 5 1 1 0 4.5kb 4.5kb

## **其它相关**

《[Elasticsearch 快速开始](https://www.cnblogs.com/cjsblog/p/9439331.html" \t "https://www.cnblogs.com/cjsblog/p/_blank)》