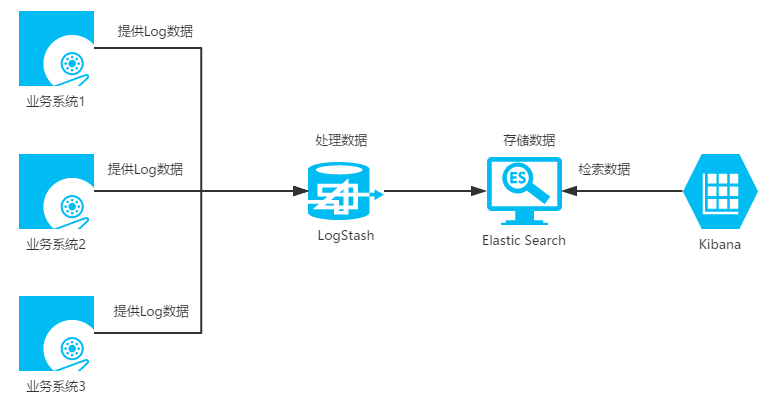
ELK

1. 什么是ELK？

ELK由Elastic Search、Logstash、Kibana三个软件组成，这三个软件都是Elastic公司开发的。https://www.elastic.co

以前，我们系统运行过程中的日志一般都是通过Log4J记录到日志文件中的。在分布式系统中，进行日志的分析、检索就很麻烦，这时候就需要用分布式日志系统。把多个系统、多个服务器上的日志汇总到日志服务器上。ELK就是一个日志服务器的套件。



LogStash是进行日志汇总、过滤的，ES是负责日志的保存和检索的，Kibana是一个图形化的查询页面。

1. 说明

ELK服务器可以注册成windows服务，但是windows下只是测试，正式生产部署要在linux下，因此也就不研究如何注册成windows服务了。

以前传统的Java+ELK的使用方式是：Java端通过Log4J记录日志，Log4J中使用SocketAppender通过网络把日志发送到LogStash，LogStash再把数据发给Elastic Search存储。

不过通过Log4j的SocketAppender直接发给Logstash的方式有漏洞，而且默认格式数据也很难看。官方已经不推荐了，Logstash也默认禁止了Log4J插件，官方建议用FileBeat。https://www.elastic.co/blog/log4j-input-logstash

1. FileBeat

有两种用法：

1. Java端通过Log4J记录日志到文件，FileBeat运行在Java端服务器上监控日志文件的变化，然后把变化的日志信息直接通过网络发给Elastic Search保存。这种情况不需要LogStash。
2. Java端通过Log4J记录日志到文件，FileBeat运行在Java端服务器上监控日志文件的变化，然后把变化的日志信息通过网络发给LogStash，LogStash再通过网络发给Elastic Search保存；

filebeat是Elastic收购的一个产品，收购前和LogStash是竞争关系， filebeat更轻量，占用资源更少，但logstash 具有filter功能，能过滤分析日志。因此如果不需要对日志进行过滤就用方法1，否则就用方法2。

1. 无论是哪种方法，都需要先配置运行ES和Kibana。
2. 安装ELK需要JDK1.8及以上版本。
3. 从官网依次下载ElasticSearch、LogStash、Kibana、FileBeat（Beats下）
4. ES启动很简单，只要运行bin目录下的 elasticsearch.bat即可，端口默认是9200。
5. Kibana也需要配置指向ES，所以需要只要修改config下的kibana.yml文件，加入

elasticsearch.url: "http://127.0.0.1:9200"

可以修改kibana.yml的server.port的值修改kibana的端口号，比如5601，

然后启动bin下的kibana.bat即可。

1. 应用中配置log4j输出日志

<dependency>

<groupId>log4j</groupId>

<artifactId>log4j</artifactId>

<version>1.2.17</version>

</dependency>

src下（放到classpath根底下）创建log4j.properties，内容如下

log4j.rootLogger = debug,stdout,drf

log4j.appender.stdout = org.apache.log4j.ConsoleAppender

log4j.appender.stdout.Target = System.out

log4j.appender.stdout.layout = org.apache.log4j.PatternLayout

log4j.appender.stdout.layout.ConversionPattern = [%-5p] %d{yyyy-MM-dd HH:mm:ss,SSS} method:%l%n%m%n

log4j.appender.drf = org.apache.log4j.DailyRollingFileAppender

log4j.appender.drf.File = d:/app.log

log4j.appender.drf.Append = true

log4j.appender.drf.Threshold = DEBUG

log4j.appender.drf.layout = org.apache.log4j.PatternLayout

log4j.appender.drf.layout.ConversionPattern = %-d{yyyy-MM-dd HH:mm:ss} [ %t:%r ] - [ %p ] %m%n

代码：

**import** org.apache.log4j.Logger;

**public** **class** Test1 {

**private** **static** **final** Logger ***logger*** = Logger.*getLogger*(Test1.**class**);

**public** **static** **void** main(String[] args) {

***logger***.debug("debug 1");

***logger***.debug("debug 1");

***logger***.debug("debug 2");

***logger***.warn("warn1");

***logger***.warn("warn2");

String s = "7ab x/6";

**try**

{

Integer.*parseInt*(s);

}

**catch**(Exception ex)

{

***logger***.error("toStringfail",ex);

}

}

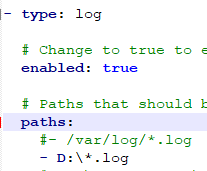
}

1. FileBeat的第一种用法

下载解压filebeat（从elastic官网的Beats模块下）到日志文件所在的服务器

修改filebeat.yml内容如下：

把type下的enabled改为true，paths中指向日志文件路径，可以用通配符d:\\*.log



增加配置：

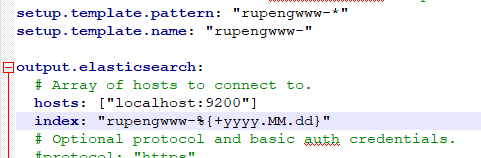
setup.template.pattern: "rupengwww-\*"

setup.template.name: "rupengwww-"

然后再output.elasticsearch:下面配置

hosts: ["localhost:9200"]

index: "rupengwww-%{+yyyy.MM.dd}"



建议不同业务系统用不同的前缀。

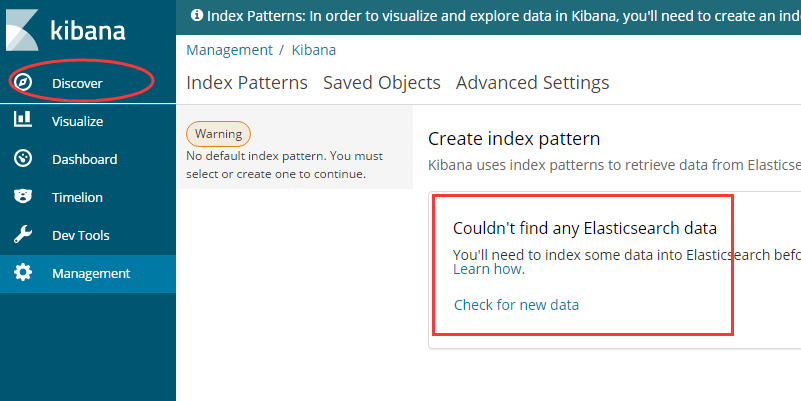
然后执行filebeat -e -c filebeat.yml启动filebeat监控

1. Kibana的使用

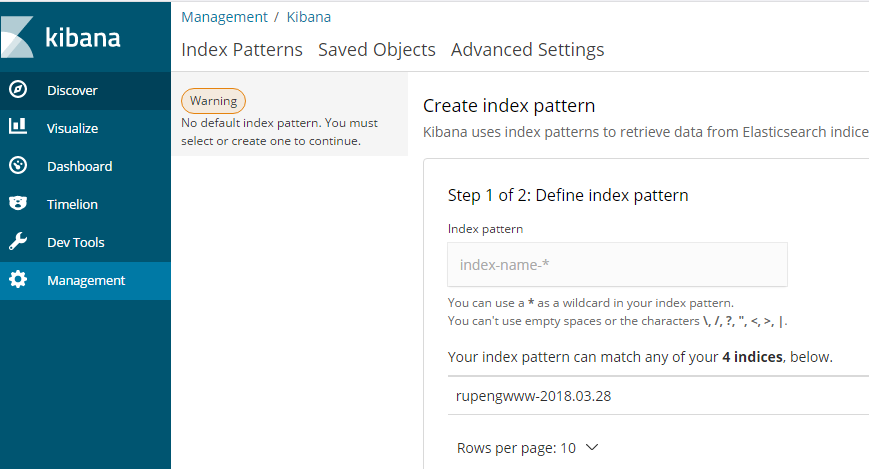
运行起来ES、Kibana，启动起来后运行Java程序生成初始数据

访问Kibana的Web页面：http://127.0.0.1:5601

点击【Discover】



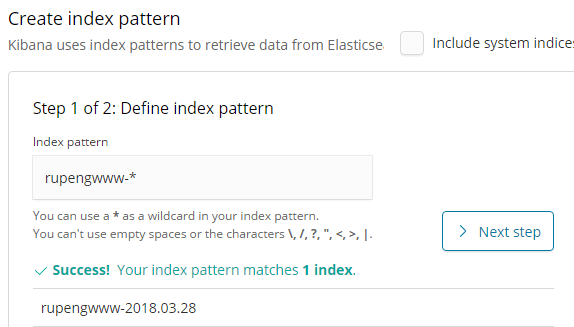
如果显示的是【Couldn't find any Elasticsearch data】，说明日志数据没有被正确写入或者没有写入数据。要解决问题最后直到写入成功，刷新后显示如下界面：



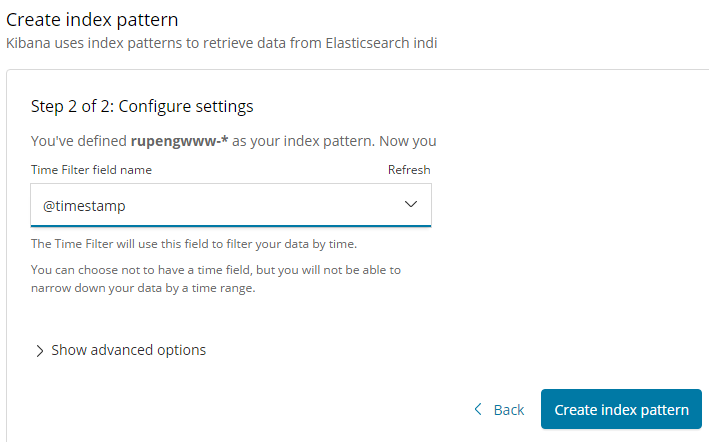
这里的【rupengwww-2018.03.28】就是filebeat写入ES的日志数据产生的索引名字。

可以访问http://127.0.0.1:9200/{索引名}/\_search?q=\*（比如http://127.0.0.1:9200/rupengwww-2018.03.28/\_search?q=\*）查看ES中的原始数据。

为日志归类，在index-name-\*中输入“rupengwww-\*”（过滤条件表示所有rupengwww-开头的索引都归为一类），然后点击【NextStep】按钮

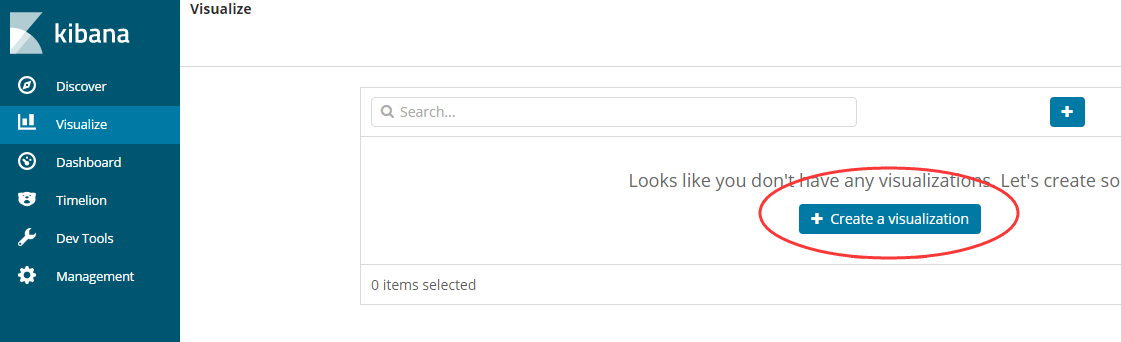


选择【@timestamp】，然后点击【Create Index Pattern】



回到Discover中选择刚才创建【rupengwww-\*】（如果有多个Filter就会有下拉选择），就可以查看日志的原始数据。

增加或者删除Filter就到Management的Index Patterns中。



查看时间线图形报表：Visual→【Create a visualization】→Time Series→TimeLion

1. FileBeat方法2的配置

logstash 稍微复杂些，需要在logstash的bin文件夹下创建 logstash.conf （需要确保文件格式是“UTF-8无BOM”）。内容如下：

input {

beats {

port => 8888

}

}

output {

elasticsearch {

hosts => "127.0.0.1:9200"

index => "rupengwww2-%{+YYYY.MM.dd}"

}

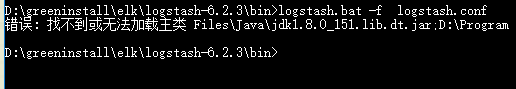
}

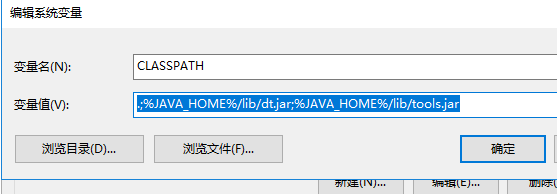
其中port => 8888表示logstash监听8888端口。

有的文档中讲的是配置一个document\_id=>"${id}"，那就会发现只保存一条数据，因为用http://127.0.0.1:9200/logstash-2018.03.27/\_search?q=\*到ES中查会发现原始数据的id保存的是 ${id}，不写document\_id就会用自动id。

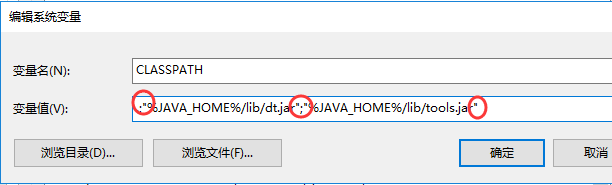
然后执行logstash.bat -f  logstash.conf

如果有下面的错误，说明环境变量配置中没有对于可能有中文、空格的路径加上""



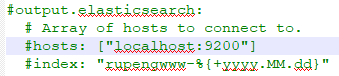


要加上双引号（注意需要是英文输入法下），修改完环境变量要重启cmd

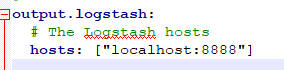


修改filebeat的配置

把output.elasticsearch相关的节点和子节点注释“#”



启用output.logstash节点，设置hosts: ["localhost:8888"]指向logstash



再执行一遍java程序生成日志

到Management的Index Patterns中增加新的Filter来过滤分类这个新数据。