ELK 使用手册

1.在10.16.33.136主机上为logstash配置项目logback需要的端口

打开/data/ELK/logstash/logstash.conf文件。

在input tag中添加如下的配置：

tcp {

type => "test"

mode => "server"

host => "10.16.33.136"

port => 4561 该端口就是logback中要用到的端口

codec => json\_lines

}

1. 在10.16.33.136主机使用docker停止原有的logstash运行的容器和镜像,

并且生成新的镜像和运行。

sudo docker stop containID

Sudo docker rm containID

Sudo docker rmi imageID

Sudo docker build -t logstash-6.4.3

Sudo docker run -it --restart=always --net=host -p 9600:9600 -v "/data/ELK/logstash:/etc/logstash/conf.d" logstash-6.4.3

3.spring boot配置使用：

<**appender name="LOGSTASH"  
 class="net.logstash.logback.appender.LogstashTcpSocketAppender"**>  
 <**destination**>10.16.33.136:4560</**destination**>  
 *<!-- encoder必须配置,有多种可选 -->* <**encoder charset="UTF-8"  
 class="net.logstash.logback.encoder.LogstashEncoder"**>  
 <**customFields**>{"appname":"owl-service"}</**customFields**>**注：appname不能有大写字母**  
 </**encoder**>  
</**appender**>

4.Kibana使用

地址：http://10.16.33.136:5601/

当logback产生log后就可以在Kibana查看。

在Management选项中进行[Index Patterns](http://10.16.33.136:5601/app/kibana" \l "/management/kibana/indices/) 。

通过 [Create Index Pattern](http://10.16.33.136:5601/app/kibana" \l "/management/kibana/index) 菜单选择要查看项目和时间的log创建index pattern。

进入Discover选择选择刚刚创建的index pattern 通过右上角的时间来查看log。