Elk搭建笔记

一、ELK搭建篇

官网地址: https://www.elastic.co/cn/products

ELK是Elasticsearch、Logstash、Kibana的简称，这三者是核心套件，但并非全部。

Logstash是一个用来搜集、分析、过滤日志的工具；Elasticsearch是实时全文搜索和分析引擎，提供搜集、分析、存储数据三大功能，但一般情况只使用该组件存储logstash过滤后的日志；Kibana是一个基于Web的图形界面，用于搜索、分析和可视化存储在 Elasticsearch指标中的日志数据。

安装环境

Liunx服务器 两台

IP：172.10.10.31 安装： elasticsearch、logstash、Kibana、elasticsearch-head

172.10.10.32 安装: logstash

安装步骤

我是在自己的电脑上下载好所有组件的压缩包上传到服务器上进行安装的。也可以直接在服务器上进行下载，看网上说的要配置elasticsearch的yum源的密钥（这个需要在所有服务器上都配置）。

1. 安装java环境(java环境必须是1.8版本以上的)

下载java：

wget http://download.oracle.com/otn-pub/java/jdk/8u131-b11/d54c1d3a095b4ff2b6607d096fa80163/jdk-8u131-linux-x64.rpm

安装java

rpm -ivh jdk-8u131-linux-x64.rpm

添加环境变量

vi /etc/profile进行配置路径

export JAVA\_HOME=jdk存放路径

export JRE\_HOME=$JAVA\_HOME/jre

export PATH=$JAVA\_HOME/bin:$PATH

export CLASSPATH=./:JAVA\_HOME/lib:$JRE\_HOME/lib”命令，

验证java是否安装成功

java -version

java version "1.8.0\_131"

Java(TM) SE Runtime Environment (build 1.8.0\_131-b11)

Java HotSpot(TM) 64-Bit Server VM (build 25.131-b11, mixed mode)

1. 分别解压elk组件压缩包，elk的安装需要创建新用户，因为elasticsearch的不能使用root用户启动。tar zxvf logstash-6.5.2.tar.gz
2. Elasticsearch安装注意事项

需要修改几个参数，不然启动会报错

vim /etc/security/limits.conf

在末尾追加以下内容（elk为启动用户，当然也可以指定为\*）

elk soft nofile 65536（无法创建本地文件,用户最大可创建文件数不够）

elk hard nofile 65536

elk soft nproc 2048（无法创建本地线程问题,用户最大可创建线程数太小）

elk hard nproc 2048

elk soft memlock unlimited（锁定内存）

elk hard memlock unlimited

继续再修改一个参数

vim /etc/security/limits.d/90-nproc.conf

将里面的1024改为2048（ES最少要求为2048）

\* soft nproc 2048

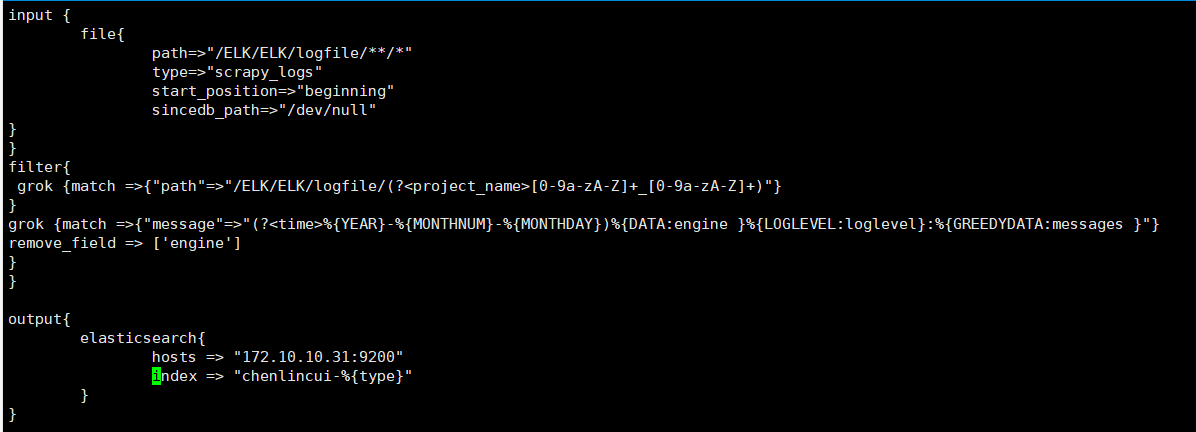
1. 启动服务

Elasticsearch启动服务：进入Elasticsearch根目录执行bin/elasticsearch，成功后如图（端口号为9200）：



kibana启动服务：进入kibana根目录执行bin/kibana

LogStash 的运行需要指定一个配置文件，来指定数据的流向，该配置文件中应指明数据来源（监听源）、输出源，根据需要可以对数据进行分析过滤格式化等操作。例如： config\_logs\_data/scrapy\_logs.conf的配置文件



写好配置文件后，

启动bin/logstash -f config\_logs\_data/scrapy\_logs.conf

1. Elasticsearch-head插件的安装

ealsticsearch只是后端提供各种api，elasticsearch-head是一款专门针对于elasticsearch的客户端工具。

elasticsearch6.0不支持命令行安装head插件，只能手动下载。

安装node.js

　这个比较容易，下载后除路径自己填写外，其他直接next就OK了。下载地址：https://nodejs.org/en/download/ 。

Grunt安装

运行head需要借助grunt命令，因此需要安装grunt， cd安装nodejs的路径）。），然后执行指令 npm install -g grunt -cli 进行安装grunt。

安装过程中国内可能因为网的原因会安装失败，修改镜像：npm config set registry <https://registry.npm.taobao.org>;

但是在安装之后启动grunt server出错

grunt-cli: The grunt command line interface. (v0.1.13)   
Fatal error: Unable to find local grunt.   
If you're seeing this message, either a Gruntfile wasn't found or grunt   
hasn't been installed locally to your project. For more information about   
installing and configuring grunt, please see the Getting Started guide:

原因是虽然安装了grunt-cli,但是在安装目录下找不到grunt

解决方法：目录下安装 npm install grunt --save-dev

启动grunt

cd 到安装elasticsearch-head的存有Gruntfile.js文件的目录下，执行grunt server命令。

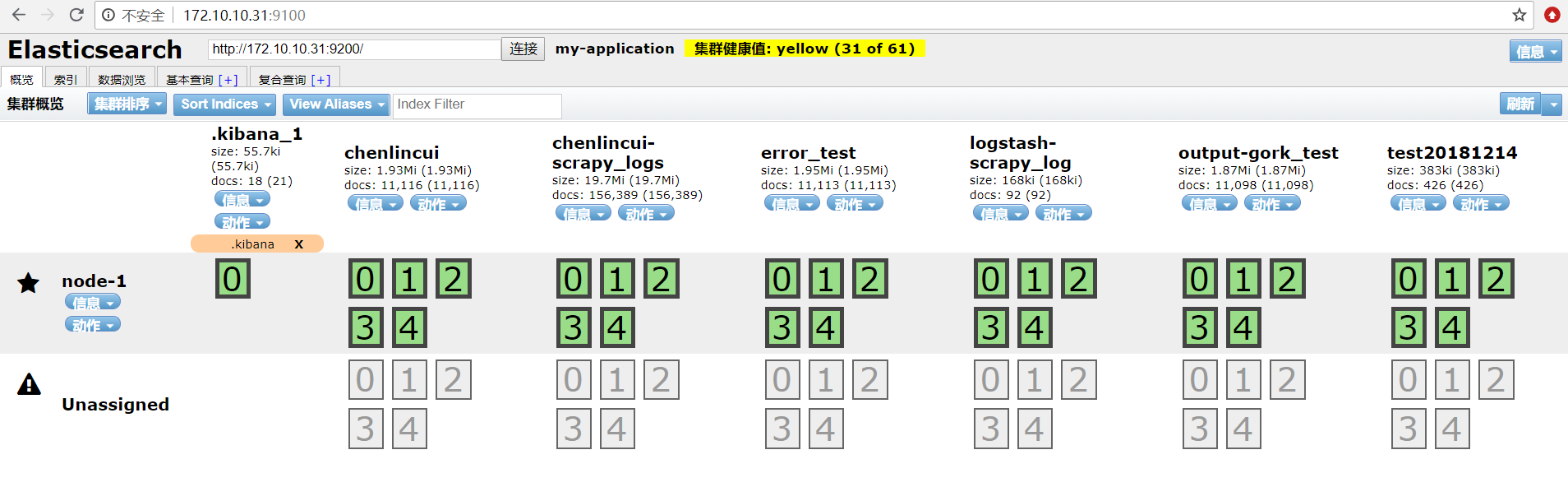
使用head等插件监控集群信息，需要打开以下配置项

# http.cors.enabled: true

# http.cors.allow-origin: "\*"

# http.cors.allow-credentials: true

安装了Elasticsearch-head的端口要改为9100，但是其监听的其实还是9200的数据。如图：



1. 远程访问

Kibana远程访问配置：kibana下的config/kibaba.yml文件中的

server.host: "localhost" 更改为server.host: "0.0.0.0" 就可以了

elasticsearch远程访问配置：

Elasticsearch的配置文件vimconfig/elasticsearch.yml找到network.host这一行。将该行最前面的#去掉，修改成network.host: 0.0.0.0。

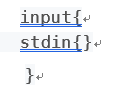
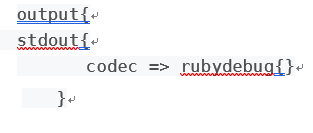
二、ELK实战篇

Elk日志分析主要是logstash的日志收集、过滤，最后将处理的数据通过kibana可视化。

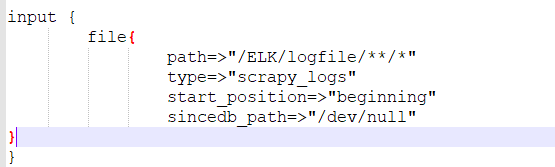
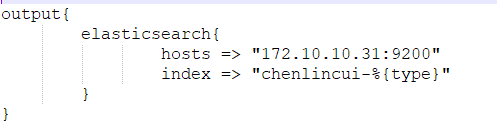
Logstash的日志收集、分析过滤主要都是通过配置文件完成的，该配置文件主要包含三个插件：input、filter、output.

logstash之input、output插件

**标准输入/输出**

**文件输入、elasticsearch输出**



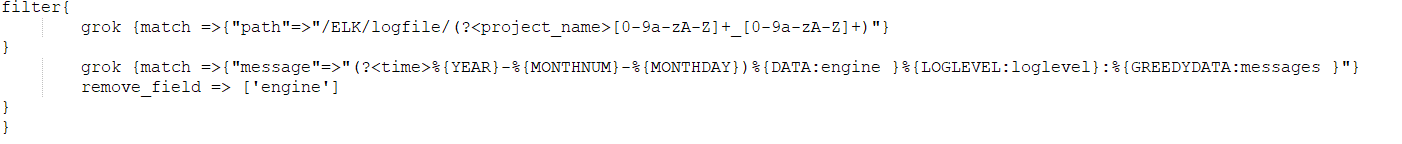


**还有很多输入、输出，比如syslog输入、redis输出等。**

logstash之filter插件

1、grok插件

grok插件有非常强大的功能，他能匹配一切数据，但是他的性能和对资源的损耗同样让人诟病。



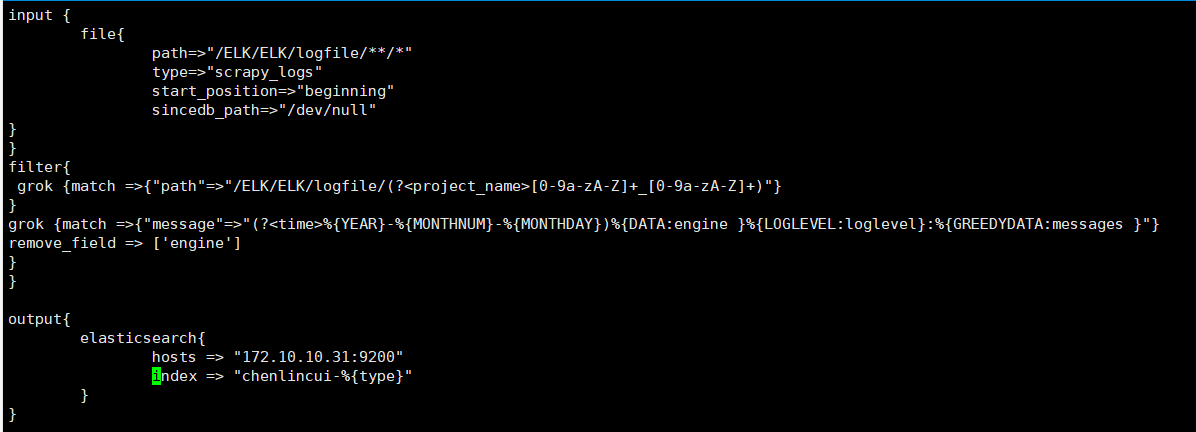
**grok模式的语法如下：**%{SYNTAX:SEMANTIC}

SYNTAX：代表匹配值的类型,例如127.0.0.1可以使用IP类型匹配。Grok内置了很多正则匹配的内容（<http://www.cnblogs.com/stozen/p/5638369.html>）

SEMANTIC：代表存储该值的一个变量名称,例如,127.0.0.1可能是请求的client地址。所以%{IP:client} 来匹配。

**自定义正则表达式语法：**(?<field\_name>the pattern here)

# scrapy日志处理，分割出项目名称（根据log路径分割）、日志的级别（message分割）、time、详细信息messages



2、mutate插件 mutate插件是用来处理数据的格式的，，或者你想把一个字符串变为数字类型（当然需要合法）。可以设置的转换类型 包括： "integer"， "float" 和 "string"。



