ELK日志收集系统安装文档

ELK简介

- ELK由ElasticSearch、Logstash和Kiabana三个开源工具组成。
- Elasticsearch是个开源分布式搜索引擎，它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制，restful风格接口，多数据源，自动搜索负载等。
- Logstash是一个完全开源的工具，他可以对你的日志进行收集、过滤，并将其存储供以后使用（如，搜索）。
- Kibana 也是一个开源和免费的工具，它Kibana可以为 Logstash 和 ElasticSearch 提供的日志分析友好的 Web 界面，可以帮助您汇总、分析和搜索重要数据日志。
-

> `ELK工作原理`：Logstash负责收集application产生的日志，并通过配置过滤规格来过滤日志信息，然后将过滤后的信息存放在ElasticSearch集群中。Kibana负责从ElasticSearch集群中查询日志信息，生成图表，在browser端以web页面展示与交互。

ELK安装

`系统环境`：CentOS6.5 Java1.8

ElasticSearch安装

1. 下载安装包---->:下载地址

2. 解压

> `tar -zxvf elasticsearch-2.1.0.tar.gz`
>
> `cd elasticsearch-2.1.0`
>
> *安装插件（可选）：*
>
> > `./bin/plugin install mobz/elasticsearch-head(head插件)`
> >
> > `./bin/plugin install lmenezes/elasticsearch-kopf(kopf插件)`

3. 编辑ES配置文件

> `vi config/elasticsearch.yml`
>
> 修改以下配置：

```
cluster.name=es_cluster
node.name=node0
path.data=/tmp/elasticsearch/data
path.logs=/tmp/elasticsearch/logs
#当前hostname或IP
```

```
network.host=192.168.1.117
network.port=9200
```

4. 启动

> `./bin/elasticsearch`
>
> **注意：以非root用户启动，否则报错**

5. 可视化

`在浏览器输入你的IP:9200或者你的IP：9200/_plugin/kopf(如果安装)或者你的IP：9200/_plugin/head(如果安装)`

Logstash安装

1. 下载安装包---->:下载地址

2. 解压

> `tar -zxvf logstash-2.1.1.tar.gz`
>
> `cd logstash-2.1.1`

3. 编辑配置文件(名字和位置可以随意，这里我放在config目录下，取名为`log4j_to_es.conf`)：

> `mkdir config`
>
> `vi config/log4j_to_es.conf`

输入以下内容：

```
# For detail structure of this file
# Set: https://www.elastic.co/guide/en/logstash/current/configuration-file-structure.html
# 输入
input {
  # For detail config for log4j as input,
  # See: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-log4j.html
  log4j {
    mode => "server"
    host => "192.168.1.117"
    port => 4567
  }
}
# 过滤规则
filter {
  # Only matched data are send to output.
}
# 输出
output {
  # For detail config for elasticsearch as output,
```

```
  # See: https://www.elastic.co/guide/en/logstash/current/plugins-outputs-elasticsearch.html
  elasticsearch {
    action => "index"          #The operation on ES
    hosts  => "192.168.117:9200"   #ElasticSearch host,  can be array.
    index  => "applog"         #The index to write data to.
  }
}
```

4. 启动

> `./bin/logstash agent -f config/log4j_to_es.conf`

Kibana安装

1. 下载安装包---->:下载地址

2. 解压

> `tar -zxvf kibana-4.3.0-linux-x86.tar.gz`
>
> `cd kibana-4.3.0-linux-x86`

3. 编辑配置文件

> `vi config/kibana.yml`

修改以下：

```
server.port: 5601
server.host: “192.168.1.117”
elasticsearch.url: http://192.168.1.117:9200
kibana.index: “.kibana”
```

4. 启动

> `./bin/kibana`

5. 可视化

在浏览器输入`192.168.1.117:5061`