链滴

ElasticStack 框架搭建

作者：bigbear

原文链接：https://ld246.com/article/1585290826489

来源网站：链滴

1. 简介

Elastic Stack是一个数据搜索、分析引擎，具有分布式、可伸缩等特点，通常用来做日志搜索服务器。

2. Elastic Stack的组件

- ElasticSearch （搜索核心）
- Kibana （数据可视化）
- Logstash （采集、清洗、转储）
- FileBeat （日志文件采集器）

3. 部署

使用7.6.1版本，注意全部组件统一版本号。

作为演示，本次使用单机部署，也就是ElasticSearch、Kibana、Logstash等部署在同一台机器并且别一个实例，生产环境下最好部署在不同的机器。ElasticSearch是搜索核心，分布式部署可以提高搜效率，数据分片可以容灾保证数据不丢失。

3.1. 环境

- Windows Server 2016 X64

3.2. 准备

- Elastic Stack 7.6.1
- JDK 8+

3.3. 部署流程

ElasticSearch首先部署，再部署其他组件

3.3.1. ElasticSearch

1. 解压文件到 C:\ELK\elasticsearch

2. 修改配置文件 config\elasticsearch.yml

```
cluster.name: my-application # 集群名称
node.name: node-1 # 节点名称
network.host: 0.0.0.0 # 服务IP地址，默认是127.0.0.1只能本机访问
http.port: 9200 # 服务端口号
cluster.initial_master_nodes: ["node-1", "node-2"]
node.data: true # 节点是否可以存储数据
node.master: true # 节点是否具有成为主节点的资格
```

1. 运行 Elasticsearch 实例

```
bin\elasticsearch.bat
```

1. 查看实例是否启动成功

用浏览器访问 http://localhost:9200/ 有实例信息就是启动成功了

3.3.2. Kibana

1. 解压文件到 C:\ELK\kibana
2. 修改配置文件 config\kibana.yml

```
server.port: 5601 # 服务端口号
server.host: "0.0.0.0" # # 服务IP地址
elasticsearch.hosts: ["http://localhost:9200"] # 连接的ElasticSearch实例
kibana.index: ".kibana"
i18n.locale: "zh-CN" # 中文简体，默认是英文
```

1. 运行 Kibana 实例

```
bin\kibana.bat
```

1. 查看实例是否启动成功

用浏览器访问 http://localhost:5601/ ，看到管理界面就是启动成功了

3.3.3. Logstash

1. 解压文件到 C:\ELK\logstash
2. 在 bin 目录创建配置文件 bin\logstash.conf

```
# 输入
input {
  beats {
      port => 5044
    }
}

# 过滤器
filter {
    dissect {
        mapping => {
            "message" => "%{Level}    %{ActionType}    %{TypeNumber}    %{CardNumber}    %{Ro
e}    %{Content}"
        }
    }
}

# 输出
output {
  elasticsearch {
    hosts => ["http://127.0.0.1:9200"]
  }
```

```
}
```

1. 运行 logstash 实例

```
bin/logstash -f logstash.conf
```

3.3.4. FileBeat

将 filebeat 部署在需要采集日志文件的机器，可以选择输出到 Logstash 做进一步的处理，也可以直输出到 Elasticsearch，这里我选择输出到 Logstash。

1. 解压文件到你喜欢的目录
2. 修改配置文件 filebeat.yml

```
- type: log
  # Change to true to enable this input configuration.
  enabled: true
  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - E:\Java\ELK\tmp\log\* # 采集的日志目录，支持通配符

#setup.kibana:

output.logstash:
  # The Logstash hosts
  hosts: ["10.8.6.160:5044"]
```

1. 启动 filebeat，开始采集日志并传输给 Logstash

```
./filebeat.exe -e
```

4. 样例日志

字段之间用 tab 符号分隔

000000　开机启动　2001　000000000　03(系统及设备维护人员)　启动成功，读写器连接正常打印机连接正常。