LEKStack安装搭建文档

1. 日志平台的结构示意图

架构说明：

多个独立的agent(Shipper)负责收集不同来源的数据，一个中心agent(Indexer)负责汇总和分析数据，在中心agent前的Broker(使用redis实现)作为缓冲区，中心agent后的ElasticSearch用于存储和搜索数据，前端的Kibana提供丰富的图表展示。

Shipper表示日志收集，使用LogStash收集各种来源的日志数据，可以是系统日志、文件、redis、mq等等；

Broker作为远程agent与中心agent之间的缓冲区，使用redis实现，一是可以提高系统的性能，二是可以提高系统的可靠性，当中心agent提取数据失败时，数据保存在redis中，而不至于丢失；

中心agent也是LogStash，从Broker中提取数据，可以执行相关的分析和处理(Filter)；

ElasticSearch用于存储最终的数据，并提供搜索功能；

Kibana提供一个简单、丰富的web界面，数据来自于ElasticSearch，支持各种查询、统计和展示；

2. 搭建部署

环境：

本机(172.16.2.64)上部署：redis, indexer agent(LogStash), ElasticSearch以及Kibana

远程测试机(172.16.2.65)上部署：shipper agent(LogStash)

Redis版本：redis-3.0.1

LogStash版本；logstash-1.4. 2

ElasticSearch版本：elasticsearch-1.4.4

Kibana版本：Kibana-4.0.1

JDK 1.7

2.1 部署redis

2.1.1部署redis

|  |
| --- |
| wget http://download.redis.io/releases/redis-3.0.1.tar.gz  tar zxvf redis-3.0.1.tar.gz -C /usr/local |

2.1.2 redis.conf 配置文件为

|  |
| --- |
| include ../redis.conf  daemonize yes  pidfile /var/run/redis\_6379.pid  port 6379  logfile /opt/logs/redis/6379.log  appendonly yes |

2.1.3 启动redis server

|  |
| --- |
| redis.server redis.conf |

2.2 部署中心LogStash

|  |
| --- |
| $ wget https://download.elasticsearch.org/logstash/logstash/logstash-1.4.2.tar.gz  $ tar zxvf logstash-1.4.2.tar.gz -C /usr/local/  $ cd /usr/local/logstash-1.4.2  $ mkdir conf logs |

2.2.1配置文件conf/central.conf

|  |
| --- |
| input {  redis {  host => "127.0.0.1"  port => 6379  type => "redis-input"  data\_type => "list"  key => "key\_count"  }  }  output {  stdout {}  elasticsearch {  cluster => "elasticsearch"  codec => "json"  protocol => "http"  }  } |

2.2.2 启动logstash

|  |
| --- |
| bin/logstash agent --verbose --config conf/central.conf --log logs/stdout.log |

启动信息

|  |
| --- |
| Using milestone 2 input plugin 'redis'. This plugin should be stable, but if you see strange behavior, n plugin milestones, see http://logstash.net/docs/1.4.1/plugin-milestones {:level=>:warn} |

2.3 部署Elasticsearch

2.3.1 下载并解压

|  |
| --- |
| wget <https://download.elasticsearch.org/elasticsearch/elasticsearch/elasticsearch-1.4.4.tar.gz>  tar zxvf elasticsearch-1.4.4.tar.gz -C /usr/local |

2.3.2 启动elasticsearch

|  |
| --- |
| bin/elasticsearch -d |

2.3.3 验证启动是否成功

|  |
| --- |
| curl -X GET http://172.16.2.76:9200 |

打印结果

|  |
| --- |
| {  "status" : 200,  "name" : "Hydron",  "cluster\_name" : "elasticsearch",  "version" : {  "number" : "1.4.4",  "build\_hash" : "c88f77ffc81301dfa9dfd81ca2232f09588bd512",  "build\_timestamp" : "2015-02-19T13:05:36Z",  "build\_snapshot" : false,  "lucene\_version" : "4.10.3"  },  "tagline" : "You Know, for Search"  } |

2.4 部署LogStash(Shipper)

2.4.1 配置与2.2步骤相同，只是配置文件不同

配置文件conf/shipper.conf的内容为

|  |
| --- |
| input {  file {  type => "type\_count"  path => ["/data/logs/count/stdout.log", "/data/logs/count/stderr.log"]  exclude => ["\*.gz", "access.log"]  }  }  output {  stdout {}  redis {  host => "172.16.2.76"  port => 6379  data\_type => "list"  key => "key\_count"  }  } |

2.4.2 启动

|  |
| --- |
| bin/logstash agent --verbose --config conf/shipper.conf --log logs/stdout.log |

打印信息

|  |
| --- |
| Using milestone 2 input plugin 'file'. This plugin should be stable, but if you see strange behavior, p plugin milestones, see http://logstash.net/docs/1.4.1/plugin-milestones {:level=>:warn}  Using milestone 2 output plugin 'redis'. This plugin should be stable, but if you see strange behavior,on plugin milestones, see http://logstash.net/docs/1.4.1/plugin-milestones {:level=>:warn} |

2.5 部署Kibana

这里我们用最新版本部署

2.5.1 下载并安装

|  |
| --- |
| wget https://download.elasticsearch.org/kibana/kibana/kibana-4.0.1-linux-x64.tar.gz  tar zxvf kibana-4.0.1-linux-x64.tar.gz |

2.5.2 修改配置文件

|  |
| --- |
| cat kibana.yml | grep elasticsearch\_url  elasticsearch\_url: "http://172.16.2.76:9200" |

2.5.3 启动Kibana

|  |
| --- |
| bin/kibana |

2.5.4 访问Kibana

|  |
| --- |
| http://localhost:5601 |

注：因为我的测试环境是docker，所以要如下访问

|  |
| --- |
| http://docker-test7.ops-chukong.com:40092/ |

打印输出

|  |
| --- |
| {"@timestamp":"2015-05-21T02:09:33.471Z","level":"info","message":"Listening on 0.0.0.0:5601","node\_env  {"@timestamp":"2015-05-21T02:11:46.577Z","level":"info","message":"GET / 200 - 23ms","node\_env":"produc"headers":{"host":"docker-test7.ops-chukong.com:40092","connection":"keep-alive","accept":"text/html,ap\*/\*;q=0.8","user-agent":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Maxi/537.36","dnt":"1","accept-encoding":"gzip,deflate","accept-language":"zh-CN"},"remoteAddress":"117.12tatusCode":200,"responseTime":23,"contentLength":0}} |

3 测试

3.0.1 向Shipper中加入如下信息

|  |
| --- |
| echo "stdout: Hi, I am Maven" >> stdout.log  echo "stderr: Hi, I like hot girls" >> stderr.log |

2.0.2 查看Logstash输出

|  |
| --- |
| {"@timestamp":"2015-05-21T02:56:16.191Z","level":"info","message":"GET /logstash-\*/\_mapping/field/\*?ignore\_unavailable=false&allow\_no\_indices=false&include\_defaults=true 200 - 8ms","node\_env":"production","request":{"method":"GET","url":"/elasticsearch/logstash-\*/\_mapping/field/\*?ignore\_unavailable=false&allow\_no\_indices=false&include\_defaults=true","headers":{"host":"docker-test7.ops-chukong.com:40092","connection":"keep-alive","accept":"application/json, text/plain, \*/\*","user-agent":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Maxthon/4.4.1.3000 Chrome/30.0.1599.101 Safari/537.36","dnt":"1","referer":"http://docker-test7.ops-chukong.com:40092/","accept-encoding":"gzip,deflate","accept-language":"zh-CN"},"remoteAddress":"117.121.57.5","remotePort":41820},"response":{"statusCode":200,"responseTime":8,"contentLength":12234}}  {"@timestamp":"2015-05-21T02:56:20.970Z","level":"info","message":"GET /logstash-\*/\_mapping/field/\*?ignore\_unavailable=false&allow\_no\_indices=false&include\_defaults=true 200 - 12ms","node\_env":"production","request":{"method":"GET","url":"/elasticsearch/logstash-\*/\_mapping/field/\*?ignore\_unavailable=false&allow\_no\_indices=false&include\_defaults=true","headers":{"host":"docker-test7.ops-chukong.com:40092","connection":"keep-alive","accept":"application/json, text/plain, \*/\*","user-agent":"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Maxthon/4.4.1.3000 Chrome/30.0.1599.101 Safari/537.36","dnt":"1","referer":"http://docker-test7.ops-chukong.com:40092/","accept-encoding":"gzip,deflate","accept-language":"zh-CN"},"remoteAddress":"117.121.57.5","remotePort":41820},"response":{"statusCode":200,"responseTime":12,"contentLength":12234}} |

3.0.3 查看redis输出

|  |
| --- |
| 1432177218.141644 [0 172.16.2.77:42452] "rpush" "key\_count" "{\"message\":\"stdout: Hi, I am Maven\",\"@version\":\"1\",\"@timestamp\":\"2015-05-21T03:00:18.136Z\",\"type\":\"type\_count\",\"host\":\"5bb5cf7b03da\",\"path\":\"/data/logs/count/stdout.log\"}"  1432177218.146501 [0 127.0.0.1:60743] "blpop" "key\_count" "0"  1432177226.151899 [0 172.16.2.77:42452] "rpush" "key\_count" "{\"message\":\"stderr: Hi, I like hot girls\",\"@version\":\"1\",\"@timestamp\":\"2015-05-21T03:00:26.147Z\",\"type\":\"type\_count\",\"host\":\"5bb5cf7b03da\",\"path\":\"/data/logs/count/stderr.log\"}" |

3.0.4 查询elasticsearch

|  |
| --- |
| {  "took" : 10,  "timed\_out" : false,  "\_shards" : {  "total" : 6,  "successful" : 6,  "failed" : 0  },  "hits" : {  "total" : 4,  "max\_score" : 0.5945348,  "hits" : [ {  "\_index" : "logstash-2015.05.21",  "\_type" : "type\_count",  "\_id" : "AU10RB4ikIXFN6Y4T2I2",  "\_score" : 0.5945348,  "\_source":{"message":"stdout: just a test message","@version":"1","@timestamp":"2015-05-21T10:18:50.155+08:00","type":"type\_count","host":"5bb5cf7b03da","path":"/data/logs/count/stdout.log"}  }, {  "\_index" : "logstash-2015.05.21",  "\_type" : "type\_count",  "\_id" : "AU10RFZnkIXFN6Y4T2I3",  "\_score" : 0.5945348,  "\_source":{"message":"stderr: just a test message","@version":"1","@timestamp":"2015-05-21T10:19:05.174+08:00","type":"type\_count","host":"5bb5cf7b03da","path":"/data/logs/count/stderr.log"}  }, {  "\_index" : "logstash-2015.05.21",  "\_type" : "type\_count",  "\_id" : "AU10ahJqkIXFN6Y4T2I4",  "\_score" : 0.30685282,  "\_source":{"message":"stdout: Hi, I am Maven","@version":"1","@timestamp":"2015-05-21T11:00:18.136+08:00","type":"type\_count","host":"5bb5cf7b03da","path":"/data/logs/count/stdout.log"}  }, {  "\_index" : "logstash-2015.05.21",  "\_type" : "type\_count",  "\_id" : "AU10ajG2kIXFN6Y4T2I5",  "\_score" : 0.30685282,  "\_source":{"message":"stderr: Hi, I like hot girls","@version":"1","@timestamp":"2015-05-21T11:00:26.147+08:00","type":"type\_count","host":"5bb5cf7b03da","path":"/data/logs/count/stderr.log"}  } ]  }  } |

Kibana 界面





