EFK说明文档

**一、功能**

启动EFK系统，测试新版本fluentd的稳定性。

**二、环境准备**

准备三台主机，其中一台主机启动es和kibana节点，剩余节点只启动es节点。

1）在EFK目录，修改docker-compose.yml文件：

|  |
| --- |
| - "ES\_PUBLISH\_HOST=192.168.43.106" #修改为本机的IP地址  extra\_hosts:  - "elasticsearch:192.168.43.106" #修改为实际的IP地址  - "elasticsearch2:192.168.43.107"  - "elasticsearch3:192.168.43.143"  volumes:  es-repo:  driver\_opts:  type: nfs  o: "addr=192.168.43.143,nolock,soft,rw,tcp,timeo=180" #选择三台主机中，一台磁盘较大的主机作为存储  device: ":/app/es-repo" |

修改完成后，使用命令"docker-compose up -d"，启动es节点和kibana节点。

（若只启动es节点，使用命令"docker-compose up -d es"）

2）进入fluentd目录，修改docker-compose文件：

|  |
| --- |
| - HOST\_NAME=192.168.43.143 #修改为本机IP地址 |

修改fluentd.conf文件：

|  |
| --- |
| hosts 192.168.43.143:9200 #(可以写多个host:port, 逗号分隔) |

修改完成后，使用命令"docker-compose up -d"，启动fluentd节点。

**三、导入日志**

在fluentd目录，查看test.sh脚本权限，使用命令"chmod u+x test.sh"赋予其执行权限。

脚本文件如下：

|  |
| --- |
| #!/bin/bash  echo "Start : `date +"%Y年%m月%d日 %H:%M:%S"`" >> my.log  for i in `seq 1 20000` #根据实际情况，可修改循环次数  do  cat 1 >> ./log/1.log  done  echo "End : `date +"%Y年%m月%d日 %H:%M:%S"`" >> my.log |

通过执行脚本，循环将文件1内的内容导入至fluentd收集目录内，然后查看kibana地址，查看日志是否正常推送。