**Logstash搭建**

版本:2.0

Victors团队

## 功能任务

Logstash负责修改输入队列中的时间字段。

## Logstash安装

由于logstash无arm版本，故本软件可能不稳定。但本软件在为期3个月的持续测试中尚未出现任何异常。

1. **适用节点：**
   1. 概括：logstash节点
   2. 数量：一台
   3. 主机名：http-nodeN(N=1,2,3,4,5,6,7,8)
   4. IP:192.168.1.N(N=11,12,13,14,16,17,18,19)
2. **Logstash下载及解压：**

本系统使用的logstash版本为5.5.1版本，下载方法为

wget <https://download.elastic.co/logstash/logstash/logstash-5.5.1.tar.gz>

tar –zxvf logstash-5.5.0.tar.gz

cd logstash-5.5.0

1. **git下载，安装，使用：**

由于git与本系统关联性不强，故省略git详细安装以及配置，树莓派安装及配置git请参考以下网址：<http://www.jianshu.com/p/f31b0a717fd1>

1. **logstash安装：**
2. 获取jffi文件：git clone https://github.com/jnr/jffi.git
3. 安装ant：sudo apt-get install ant
4. 进入jffi文件夹
5. 编译jffi文件并回到logstash主目录

编译命令：ant jar

1. 删除vendor/jruby/lib/jni/arm-Linux所有文件

rm –r vendor/jruby/lib/jni/arm-Linux

1. 复制jffi/build/jni/libjffi-1.2.so到logstash/vendor/jruby/lib/jni/arm-Linux目录下

cp jffi/build/jni/libjffi-1.2.so logstash/vendor/jruby/lib/jni/arm-Linux

1. 安装完成。
2. **logstash测试：**

./bin/logstash –e “input{stdin{}}output{stdout{}}”

若产生输入回显，即表示logstash安装成功。

## 服务启动

~/logstash/bin/logstash –f ~/logstash/conf/logstash.conf

## 注意事项：

* 1. 本配置文件为本系统的配置文件，已经包含向es中写入数据的部分，故直接运行时若es未开始，只会导致开启失败；
  2. 本系统中logstash文件夹放置于/home/pi目录下（其它位置也可）；
  3. 此处的服务启动方法指该项功能的启动方式，系统具体的调用方式参见构建书综合功能部分相关源码。