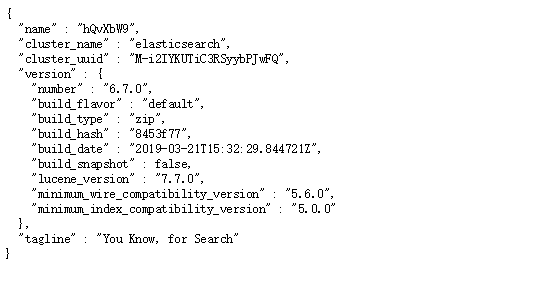
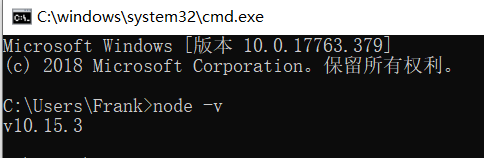
# ELK使用笔记

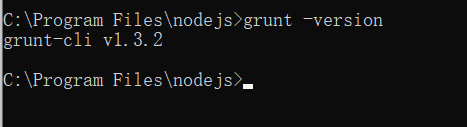
1. 安装jdk，至少1.8以上的版本，下载地址：<https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>；
2. 配置java环境变量，参考地址：<https://jingyan.baidu.com/article/f96699bb8b38e0894e3c1bef.html>；
3. 下载ELK，ElasticSearch（ES）、Logstash和Kibana，下载地址：<https://www.elastic.co/downloads/>；
4. 安装ES，cmd进入elasticsearch的bin目录，运行elasticsearch-service install，安装ES服务；运行 elasticsearch-service manager,管理配置ES，点击Start启动服务，下方的Startup type设置为Automatic最好；至此，ES服务安装配置基本完成。
5. 打开浏览器，输入http://localhost:9200/，进行验证，没有出错，返回一串json数据表示安装成功。



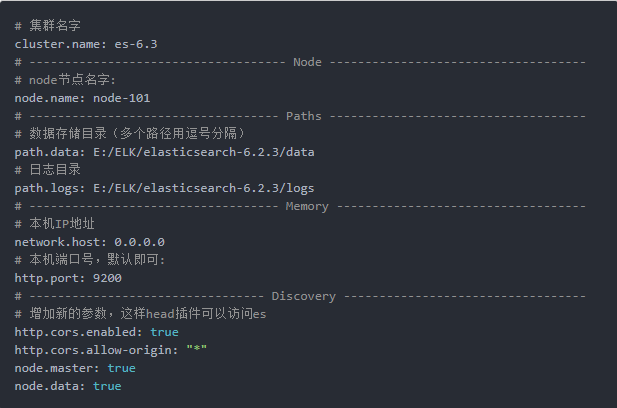
1. 下载nodejs，下载地址：<https://nodejs.org/en/>；下载完成安装，一直next即可，保持默认选项；
2. Cmd进入dos命令界面，执行node -v查看是否成功；



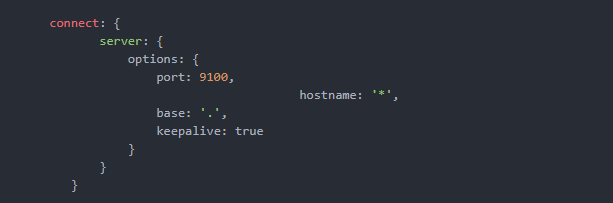
1. 在nodejs目录下执行 npm install -g grunt-cli 安装grunt ，-g代表全局安装，安装路径为C:\Users\yourname\AppData\Roaming\npm，安装完成后执行grunt -version查看是否安装成功，会显示安装的版本号。



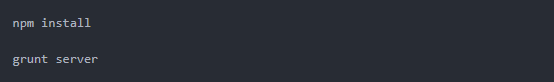
1. 修改config目录下的elasticsearch.yml文件，如下所示：



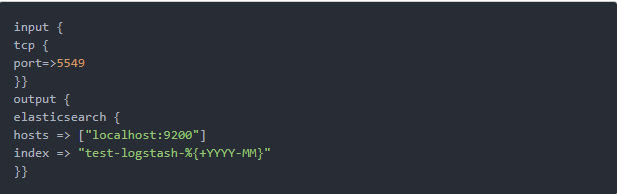
1. 重新启动ES服务，这个可以在serrvices.msc上启动，也可在bin目录下输入elasticsearch-service start启动。
2. 把head的源码clone过来，在此之前需要在[git官网](https://link.jianshu.com/?t=https%3A%2F%2Fgit-scm.com%2Fdownload%2Fwin)安装git，然后在ES的bin目录下执行git clone [git://github.com/mobz/elasticsearch-head.git](https://link.jianshu.com/?t=git%3A%2F%2Fgithub.com%2Fmobz%2Felasticsearch-head.git)。
3. 在Gruntfile.js修改head插件源码，找到connect的地方，修改如下:



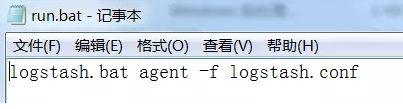
1. 在elasticsearch-head目录下运行，下面的命令：



1. 输入localhost:9100，可查看集群状态,至此ES成功安装。
2. 在logstash文件夹的bin目录里新建logstash.conf配置文件，具体内容如下，具体参数可以自定义：

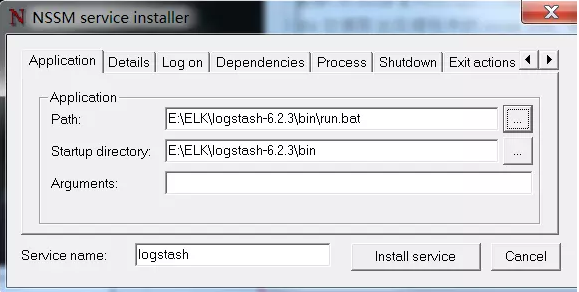


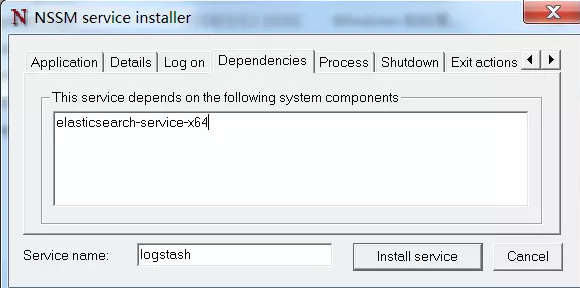
1. 在bin目录中新建logstash启动文件run.bat,内容如下：



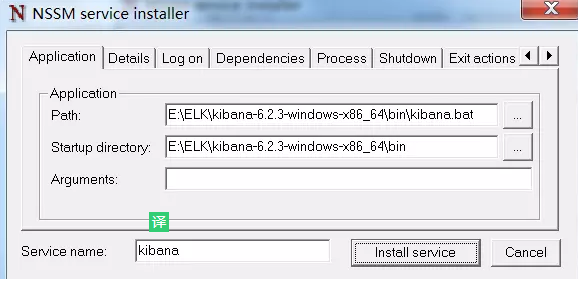
1. 下载nssm，下载地址：<http://nssm.cc/download>；根据操作系统的位数是32还是64，取出对应的nssm.exe，放入bin目录下。
2. 安装logstash到windows服务：从nssm官网下载nssm压缩包，根据操作系统是32位还是64位提取出压缩包中的nssm.exe，拷贝到logstash的bin目录下，在cmd中运行nssm install logstash，出现安装界面并填写相应的内容,在依赖(dependencies)里面根据填写如下内容（注意：Java是32位的后缀是x86,64位的是x64）。添加依赖的原因是，logstash的输出配置的是Elasticsearch，如果Elasticsearch没有启动，logstash无法正常工作。

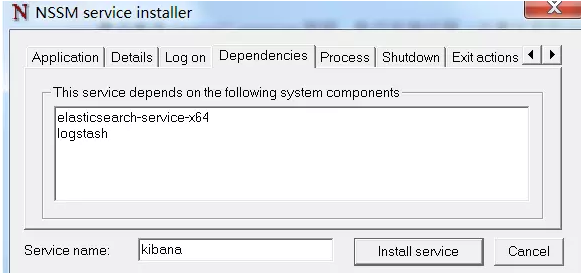






1. 最后单击install service按钮，执行安装过程（注意这里若出现警告的话，选择允许执行全部操作）。
2. 安装Kibana服务和logstash服务步骤基本相同，将nssm.exe拷贝到kibana的bin目录下，在cmd中运行nssm install kibana，填写如下内容,最后单击install service按钮，执行安装过程：





1. 在cmd中运行services.msc打开windows服务，依次启动如下服务：

Elasticsearch->Logstash->Kibana

在浏览器中输入：http://localhost:5601/ ，如果出现如下界面，表示服务启动成功：

1. 至此，所有服务安装完成，平台搭建完成，后续集群的部署还需要在ELK的各个配置文件中进行详细的配置。