根据《ELK 产品支持的平台和软件》选定你所要安装的版本。这里将安装elasticsearch最新版本2.0.0。

**1. jdk**

elasticsearch只支持[Oracle](http://www.ttlsa.com/oracle/) java 和 OpenJDK。

在这里不再重复了，参见《ELK 部署指南》详细的不能再详细了。搞不定跟帖说明吧。

**2. 安装**

elasticsearch 2.0.0版本不能以root用户启动。

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | # wget -c https://download.elastic.co/elasticsearch/release/org/elasticsearch/distribution/tar/elasticsearch/2.0.0/elasticsearch-2.0.0.tar.gz  # tar zxvf elasticsearch-2.0.0.tar.gz -C /usr/local  # useradd --system --shell /sbin/nologin elasticsearch  # chown -R elasticsearch.elasticsearch /usr/local/elasticsearch-2.0.0  # chown -R elasticsearch.elasticsearch /data/ttlsa.com/elasticsearch  # cd /usr/local/elasticsearch-2.0.0  # vi config/elasticsearch.yml  cluster.name: ttlsa-es  node.name: ${HOSTNAME}  path.data: /ttlsa/db/elasticsearch  bootstrap.mlockall: true  bootstrap.max\_open\_files: true  network.host: 10.6.7.12  # su - elasticsearch -c "/usr/local/elasticsearch-2.0.0/bin/elasticsearch -d" |

如果有报错，请查看下elasticsearch日志，养成查看日志的好习惯。

目录结构说明如下：

| **Type** | **Description** | **Location** |
| --- | --- | --- |
| **home** | elasticsearch安装的目录 | {extract.path} |
| **bin** | elasticsearch二进制脚本目录 | {extract.path}/bin |
| **conf** | 配置文件目录 | {extract.path}/config |
| **data** | 数据目录 | {extract.path}/data |
| **logs** | 日志目录 | {extract.path}/logs |
| **plugins** | 插件目录 | {extract.path}/plugins |

{extract.path}是elasticsearch zip或者tar.gz包解压的目录。elasticsearch包解压出来就可以使用。

**3. 配置**

**环境变量**

在elasticsearch启动脚本中，通过JAVA\_OPTS传递给JVM启动，其中最重要的是通过-Xmx来控制进程使用的最大的内存，通过-Xms来控制进程分配的最小内存。这两个对性能至关重要的，通常这两者设置为一样大小。

多数情况下，不要去改变JAVA\_OPTS的设置，要更改JVM设置或参数可通过ES\_JAVA\_OPTS环境变量来进行。

ES\_HEAP\_SIZE 环境变量设置elasticsearch java进程分配的内存，将最大值和最小值设置为一样，默认情况下ES\_MIN\_MEM=256m，ES\_MAX\_MEM=1g。

建议将ES\_MIN\_MEM和ES\_MAX\_MEM设置为相同的值，并启用mlockall。

**系统配置**

文件描述符

这个一般会继承系统的设置。为了查看进程可以打开了多少文件数，可以将 -Des.max-open-files设置为true。可以通过node API进行查看：

[](http://www.ttlsa.com/wp-content/uploads/2015/11/elk3.jpg)

[](http://www.ttlsa.com/wp-content/uploads/2015/11/elk-2.jpg)

虚拟内存

elasticsearch默认使用hybrid mmapfs / niofs目录存储索引。系统默认的mmap数可能太低，会导致内存溢出。在[Linux](http://www.ttlsa.com/linux/)上，需要在/etc/sysctl.conf文件中设置vm.max\_map\_count=262144。

内存设置

禁用swap。云主机默认都是禁用的。

配置swappiness。将vm.swappiness设置为0。

mlockall 尽可能的将进程锁定在内存中，防止elasticsearch内存被swap出。在elasticsearch.yml文件中设置bootstrap.mlockall: true。

如果设置了bootstrap.mlockall: true，而通过node API查看是fail的值，原因可能是:

1. 没有权限  
   在/etc/security/limits.conf文件中设置  
   elasticsearch soft memlock unlimited  
   elasticsearch hard memlock unlimited
2. 临时目录通常是/tmp以noexec选项挂载的，可以另指一个临时目录解决，./bin/elasticsearch -Djna.tmpdir=/path/to/new/dir。

**elasticsearch 设置**

elasticsearch配置文件位于ES\_HOME/config目录中。该目录中有两个文件elasticsearch.yml配置elasticsearch不同模块，logging.yml配置elasticsearch日志。配置格式是YAML。如果使用json格式，需要将elasticsearch.yml重命名为elasticsearch.json，同时，需要将文件中的配置参数转换成json格式。

elasticsearch.yml配置内容如下：



|  |  |
| --- | --- |
| 1  2  3  4  5  6 | cluster.name: ttlsa-es  node.name: ${HOSTNAME}  path.data: /ttlsa/db/elasticsearch  bootstrap.mlockall: true  bootstrap.max\_open\_files: true  network.host: 10.6.7.12 |

数据目录可以设置为多个如：path.data: ["/ttlsa/db/elasticsearch","/ttlsa/db/elasticsearch2"] 或者 path.data: /ttlsa/db/elasticsearch, /ttlsa/db/elasticsearch2。

如果想以主机名命令节点名称，同时，该服务器上只运行单个elasticsearch实例，可以设置为${HOSTNAME}变量，将从环境变量中获取主机名。也可以设置成${prompt.text}，在启动时，需要键入名称。

也可以通过使用ES\_JAVA\_OPTS或者向elasticsearch命令传递参数，如：



|  |  |
| --- | --- |
| 1 | # bin/elasticsearch -Des.network.host=127.0.0.1 |

上面配置完，并成功启动后，可以通过http://your-ip-address:9200访问了。

前面内容留了一个坑，后续再说了。