章节五 项目实战系列之阿里云服务器部署ELK，采集业务日志和分析

19、项目实战系列之《采集业务应用日志》配置

简介：选择日志源，配置logstash采集并输送到elasticSeach

常见问题解决

1、JVM内存溢出导致的 ES或者Logstash服务启不来，报错 insufficient memory

解决：升级机器的内存和CPU；

或者改elasticSeach和logstash的JVM.option，最大堆内存xmx和初始堆内存xms

2、ES启动报错

seccomp unavailable: CONFIG\_SECCOMP not compiled into kernel, CONFIG\_SECCOMP and CONFIG\_SECCOMP\_FILTER are needed

修改elasticsearch.yml 添加一下内容

bootstrap.memory\_lock: false 为了避免内存和磁盘之间的swap

bootstrap.system\_call\_filter: false

3、ERROR: bootstrap checks failed

max virtual memory areas vm.max\_map\_count [65530] is too low, increase to at least

临时设置：sudo sysctl -w vm.max\_map\_count=262144

永久修改：

修改/etc/sysctl.conf 文件，添加 “vm.max\_map\_count”设置

并执行：sysctl -p