CentOS7.9-ELK 日志分析镜像使用帮助文档

1、镜像环境说明

镜像版本说明 操作系统： CentOS7.9 64 位
Java 运行环境（CentOS 7.9 64 位 | kibana 6.2.4 | elasticsearch 6.2.4 | logstash 6.2.4 | nginx 1.16）

1.ELK 介绍
（1）ELK 是三个开源软件的缩写，分别表示：Elasticsearch , Logstash, Kibana , 它们都是开源软件。新增了一个 FileBeat，它是一个轻量级的日志收集处理工具(Agent)，Filebeat 占用资源少，适合于在各个服务器上搜集日志后传输给 Logstash，官方也推荐此工具。。
（2）Elasticsearch 是个开源分布式搜索引擎，提供搜集、分析、存储数据三大功能。它的特点有：分布式，零配置，自动发现，索引自动分片，索引副本机制，restful 风格接口，多数据源，自动搜索负载等。
（3）Logstash 主要是用来日志的搜集、分析、过滤日志的工具，支持大量的数据获取方式。一般工作方式为 c/s 架构，client 端安装在需要收集日志的主机上，server 端负责将收到的各节点日志进行过滤、修改等操作在一并发往 elasticsearch 上去

1.2 镜像安装说明

镜像环境里相应软件的安装，是基于 CentOS 7 纯净版版的官方软件包安装配 置，系统安全策略配置，系统调优、优化了相应功能。

在镜像环境中，所有软件包都是使用源码手工安装完成，您可以自由根据需 求在 CentOS 7.9 系统中做自定义服务配置，安装后的环境跟全部属于默认配置。

1.3 软件默认配置：
Nginx 配置文件路径：/etc/nginx/nginx.conf
Kibana-nginx 配置文件路径：/etc/nginx/conf.d/kibana.conf
elasticsearch-nginx 配置文件路径：/etc/nginx/conf.d/elasticsearch.conf
Kibana 配置文件：/etc/kibana/kibana.yml
elasticsearch 配置文件：/etc/elasticsearch/elasticsearch.yml

3、软件目录及配置列表

所有软件都采用源码方式安装
elasticsearch 端口 9200，
kibana 端口 5601；
Nginx 端口 80

4、软件操作命令汇总

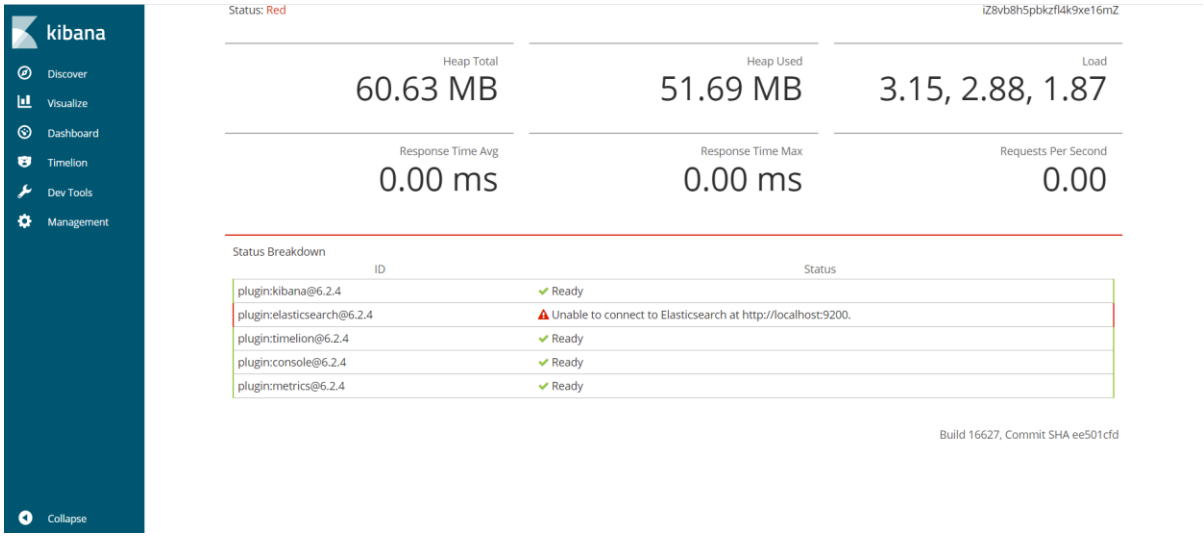
elasticsearch：systemctl start|stop|restart elasticsearch
Nginx：systemctl start|stop|restart nginx
kibana：systemctl start|stop|restart kibana
Logstash：systemctl start|stop|restart logstash

5、登录地址

Kibana 登录地址：http://ip:5601 账号：admin 密码：admin

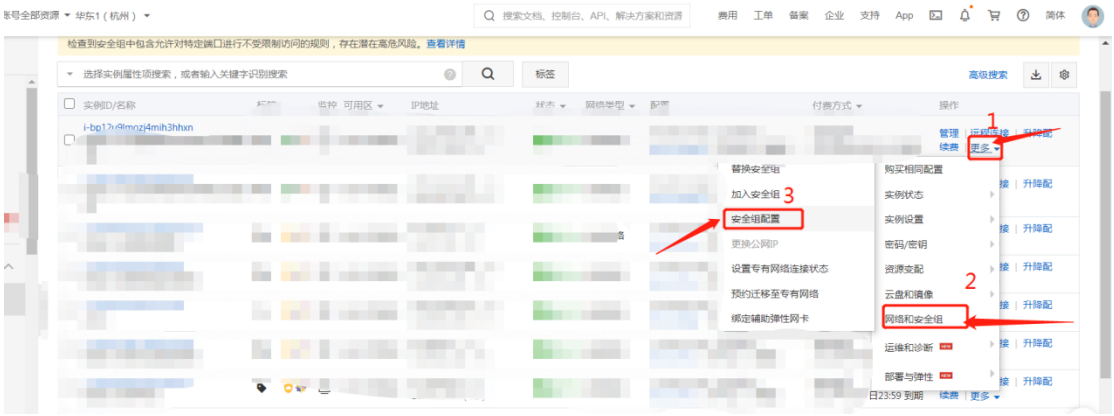
5、验证

kibana 验证页面：http://ip:5601

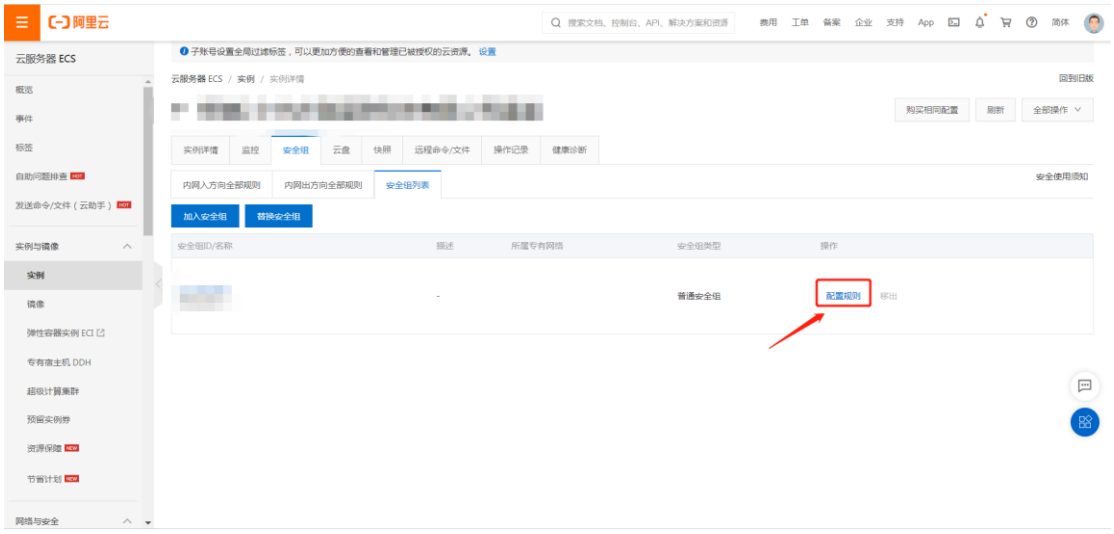


6、阿里云开放安全组

如图步骤依次点击到安全组配置



点击配置规则



点击公网入方向，点击手动添加，输入端口以及授权对象的 ip 点击保存即可

7、注意！！！1

如果三项服务都需要开启，至少要 6G 内存，否则运行不起来！！！

【公司简介】

北京众合云创科技有限公司，以技术服务为核心的技术性服务商，公司技术实力雄厚，企业核心人员，来自于 BTA，拥有丰富的行业经验，以及扎实的技术功底，以及高效的团队管理经验。公司从软件定制开发，到后期安全运维服务，全方位为客户提供解决方案。节约客户成本，提高服务质量。

【声明】

1、镜像中如有收费软件，请根据软件官方说明购买使用版权，因版权问题产生的纠纷本公司概不负责。

2、 镜像操作系统为公司定制，并经过反复测试验证，请参照商品详情中信息使用，免费镜像为客户体验使用，收费镜像为镜像制作费 用，除镜像本身默认环境问题，均不含任何人工技术支持。

3、部分付费镜像有安全加固，但不保证服务器绝对安全，互联网中不存在绝对安全的服务器，请做好代码安全，并培养良好的使用习惯。

【售后问题】

1、如有软件不能正常使用的情况请联系在线技术支持；

2、如需在线技术支持，配置、调试、故障排查等参照本公司服务类商品定价，下单后联系技术支持；

【售后支持范围】

售后服务：初始环境不能正常使用；如有任何配置修改，不在售后支持范围；

售后服务时间：周一至周六 9：00—20：00 。

售后客服联系方式：15810196073　　邮箱：hu.tang@waoqi.com

业务范围：服务器环境配置，故障排查（不含程序自身问题），数据库配置更改，数据库权限、账户，数据迁移，程序迁移，数据库故障 排查等；

费用范围：详情参照本公司服务类商品定价，或咨询在线技术支持。