ELK Stack

1. 什么是ELK？
   1. E：Elasticsearch-数据存储、分析
   2. L：LogStash-日志采集
   3. K：Kibana-日志展示
2. Why ELK？
   1. 开发人员不能登录生产服务器查看日志
   2. 一个应用可能分布于多台服务器，难以查找
   3. 同一台服务器可能部署多个应用，日志分散难以管理
   4. 会产生大量磁盘IO，可能会占用大量磁盘空间，严重时可能会造成节点宕机。
   5. 查询速度慢，不支持日志分析（比如想统计慢查询语句，查询）。
3. ES集群：
   1. 部署
      1. 操作系统：CentOS 7
      2. Java：JDK 1.8
      3. Elasticsearch：7.6.2
      4. LogStash：7.6.2
      5. Kibana：7.6.2
   2. 集群：
      1. 查看网卡信息：节点应配置正确的ip地址，CentOS中通过ifconfig查看自己的网卡和ip地址相关信息。
      2. 修改Ip地址：Linux种万物皆文件，系统的网卡信息保存在cd /etc/sysconfig/network-scripts/目录下，vi 你的网卡，修改对应的ip地址并保存，最后使用service network restart使配置生效。
   3. 配置：
      1. Cluster：

cluster.name：集群名称，集群唯一，其他节点通过cluster.name发现集群。

* + 1. Node：

node.name：节点名称，其他节点可通过node.name发现节点，默认是机器名。

* + 1. Memory：

bootstrap.memory\_lock: true：禁用swap，**生产环境必须设置为true**。

* + 1. Network：
       1. network.host：当前节点绑定的Ip地址，通常为当前服务器的ip地址。
       2. http.port：当前节点的服务端口号[9200,9300)
       3. transport.port：当前节点的通讯端口号[9300,9400)
    2. Discovery：
       1. discovery.seed\_hosts：集群中master的候选节点地址数组，可以配置ip+端口或者节点名称，

比如：discovery.seed\_hosts: ["172.16.10.184:9300", "172.16.10.185:9300"]

* + - 1. cluster.initial\_master\_nodes：集群初始master节点。

如：cluster.initial\_master\_nodes: ["node-4"]，集群启动首先会选举node-4为master节点

* + 1. 跨域：

http.cors.enabled: true

http.cors.allow-origin: "\*"

* + 1. 角色：

node.master: true 当前节点是master的候选节点

node.data: false 当前节点不是数据节点

* + 1. 单节点发现：开发模式，会绕过引导检查，生产环境能设置单节点发现。

discovery.type=single-node

* 1. Paths：切忌使用默认位置，当ES升级时会造成数据丢失。当多个节点共享同一台服务器时，不能使用相同的路径。
     1. path.data：数据储存路径，多个位置用逗号隔开
     2. path.logs：日志储存路径

[https://www.elastic.co/guide/en/elasticsearch/reference/7.7/modules-network.html#advanced-network-settings](https://www.elastic.co/guide/en/elasticsearch/reference/7.7/modules-network.html" \l "advanced-network-settings)

<https://www.elastic.co/guide/en/elastic-stack-get-started/7.6/get-started-docker.html>

ES 集群

基于OS

基于 Docker

Logstash