**Docker搭建EFK手册**

1. **部署所需资源**
2. 所需镜像
   1. elasticsearch:7.11.1
   2. elastic/filebeat:7.11.1
   3. kibana:7.11.1
3. 配置文件
   1. elasticsearch/elasticsearch.yml:/usr/share/elasticsearch/config/elasticsearch.yml
   2. filebeat/filebeat.yml:/usr/share/filebeat/filebeat.yml
   3. kibana/config/kibana.yml:/usr/share/kibana/config/kibana.yml
4. 持久化数据
   1. elasticsearch/data/:/usr/share/elasticsearch/data/

elasticsearch/logs/:/usr/share/elasticsearch/logs/

* 1. filebeat/logs/:/usr/share/filebeat/logs/
  2. kibana/data/:/usr/share/kibana/data/

kibana/logs/:/usr/share/kibana/logs/

**二、部署步骤**

解压安装包，进入解压目录

# tar -zxvf efk.tar.gz

# cd efk/

1. elasticsearch部署
   1. 更新配置文件elasticsearch/elasticsearch.yml

cluster.name: "docker-cluster"

network.host: 0.0.0.0

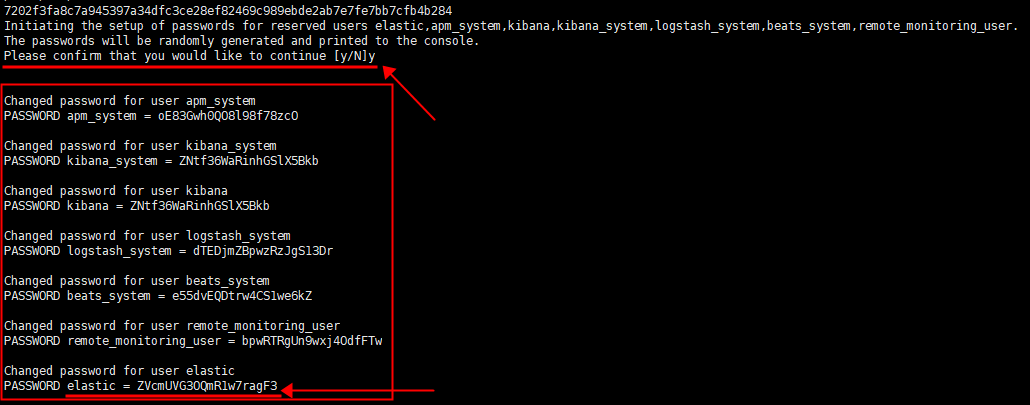
xpack.security.enabled: true

xpack.security.transport.ssl.enabled: true

* 1. 启动容器

# ./run-elasticsearch.sh

根据提示输入 y 并记录初始化密码



1. filebeat部署
   1. 更新配置文件

根据实际信息更新filebeat/filebeat.yml中的elasticsearch 地址及账号密码

filebeat.config:

modules:

path: ${path.config}/modules.d/\*.yml

reload.enabled: false

processors:

- add\_cloud\_metadata: ~

- add\_docker\_metadata: ~

filebeat.inputs:

- type: udp

enabled: true

max\_message\_size: 10KiB

host: "0.0.0.0:8000"

fields:

type: udp

setup.kibana:

host: "localhost:5601"

output.elasticsearch:

hosts: ["localhost:9200"]

# 开启xpack认证后开启

username: "elastic"

password: "admin123456"

logging.level: info

logging.to\_files: true

logging.files:

path: /usr/share/filebeat/logs

name: filebeat

keepfiles: 7

permissions: 0644

* 1. 启动容器

# ./run-filebeat.sh

1. kibana部署
   1. 更新配置文件

根据实际信息更新filebeat/filebeat.yml中的elasticsearch 地址及账号密码

#

# \*\* THIS IS AN AUTO-GENERATED FILE \*\*

#

# Default Kibana configuration for docker target

server.name: kibana

server.host: "0"

elasticsearch.hosts: [ "http://localhost:9200" ]

elasticsearch.username: "elastic"

elasticsearch.password: "admin123456"

kibana.index: ".kibana"

monitoring.ui.container.elasticsearch.enabled: true

xpack.monitoring.collection.enabled: true

#存储持久化数据的位置

path.data: /usr/share/kibana/data

# 开启中文

i18n.locale: "zh-CN"

#存储日志的文件设置

logging.dest: /usr/share/kibana/logs/kibana.log

logging.json: true

#是否只输出错误日志信息

logging.quiet: false

logging.rotate:

enabled: true

#日志文件最大大小

everyBytes: 10485760

#保留的日志文件个数

keepFiles: 7

logging.timezone: UTC

logging.verbose: true

* 1. 启动容器

# ./run-filebeat.sh

打开kibana页面进行配置

