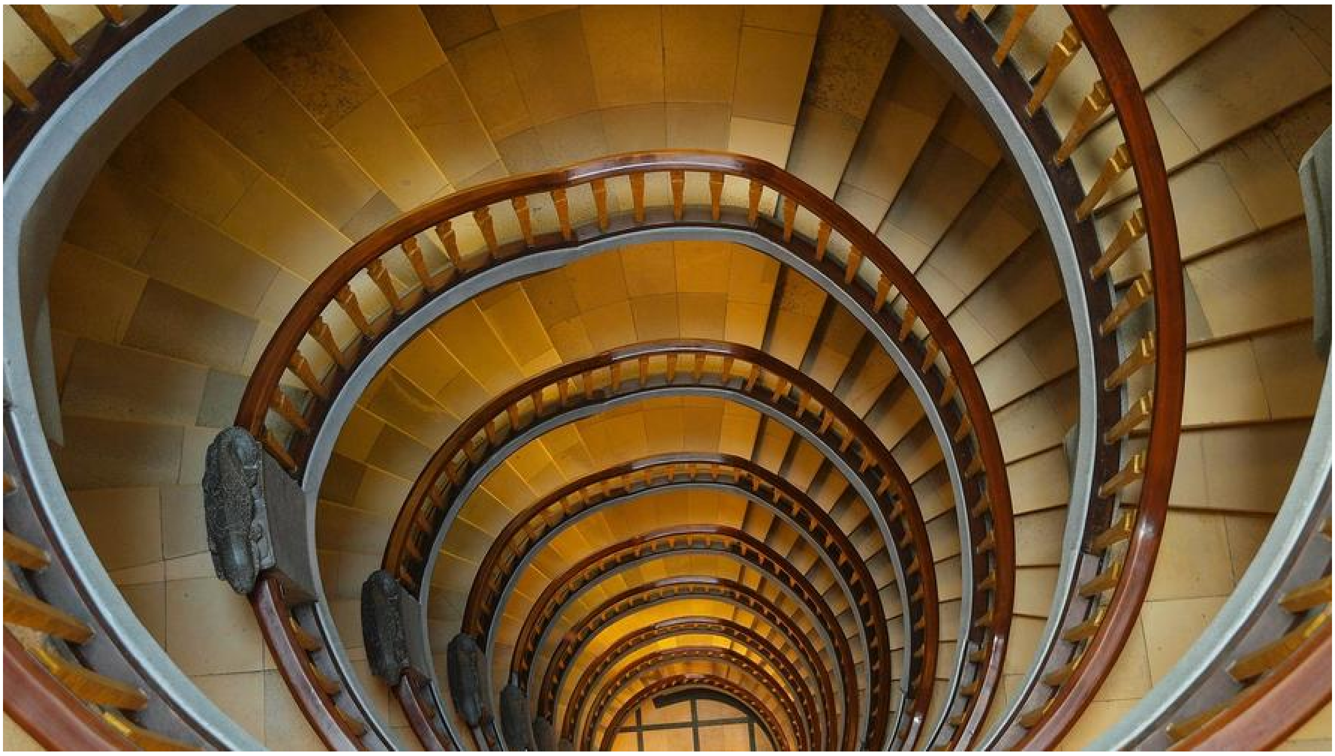
链滴

ELK 日志平台 logstash 和 filebeat

作者：opsxdev
原文链接：https://ld246.com/article/1644336061011
来源网站：链滴



ELK日志平台logstash和filebeat

1.安装 Java 环境

- 查看当前环境是否自带 JDK，需要卸载旧版本

```
[root@tike ~]# rpm -qa | grep jkd     //查看
[root@tike ~] rpm -e | grep java      //删除
# 卸载 -e --nodeps 强制删除
[root@tike ~]# rpm -e --nodeps jdkxxxxxxxxxxxxxxxxx
```

- 安装配置 java-1.8-openjdk 环境

```
[root@tike ~]# yum -y install java-1.8.0-openjdk
[root@tike ~]# yum install -y java-1.8.0-openjdk-devel
[root@tike ~]# java -version
openjdk version "1.8.0_302"
OpenJDK Runtime Environment (build 1.8.0_302-b08)
OpenJDK 64-Bit Server VM (build 25.302-b08, mixed mode)

// 不需要手工加
[root@tike ~]# vi /etc/profile
# java  environment
JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64/jre
PATH=$PATH:$JAVA_HOME/bin
CLASSPATH=.:$JAVA_HOME/lib
export JAVA_HOME CLASSPATH PATH


[root@tike ~]# source /etc/profile
```

原文链接：ELK 日志平台 logstash 和 filebeat

2.安装 logstash

配置yum源

```
cat >  /etc/yum.repos.d/logstash.repo  << EOF
[logstash-6.x]
name=Elastic repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

导入Elasticsearch PGP密钥

```
rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

安装logstash

```
yum install logstash -y
```

启动服务

```
[root@logstash ~]# systemctl start logstash
[root@logstash ~]# systemctl enable logstash
[root@logstash ~]# systemctl status logstash
```

3.添加配置文件logstash.conf

配置文件

```
input{
  kafka{
    bootstrap_servers => "192.168.7.223:9092,192.168.7.224:9092,192.168.7.227:9092"
    topics_pattern  => "onecloud-.*"
    consumer_threads => 5
    decorate_events => true
    codec => "json"
    auto_offset_reset => "latest"
    group_id => "bjo-ops-logstash"
  }
}
output {
    elasticsearch {
        hosts => ["192.168.7.232:9200", "192.168.7.231:9200", "192.168.7.229:9200"]
        # index => "%{[fields][source]}"   #直接在日志中匹配，索引会去掉额外标记onecloud
        index => "%{[@metadata][kafka][topic]}"  # 以topic建索引
        #flush_size => 20000
        #idle_flush_time => 10
        #sniffing => true
        #template_overwrite => false
```

原文链接：ELK 日志平台 logstash 和 filebeat

```
    }
}
```

4.检测配置文件是否正确

```
[root@logstash ~]# /usr/share/logstash/bin/logstash -t --path.settings /etc/logstash/  --verbose
Sending Logstash's logs to /var/log/logstash which is now configured via log4j2.properties
Configuration OK
```

5.filebet配置文件

查看配置文件内容/etc/filebeat/filebeat.yml，写入Kafka

```
filebeat.prospectors:

- input_type: log
  encoding: GB2312
#  fields_under_root: true
  fields:
    # serverip: 192.168.1.10
    logtopic: messages
  enabled: True
  paths:
        - /var/log/messages
  multiline.pattern: '^\['  #日志报错过滤
  multiline.negate:  true
  multiline.match: after
  tail_files: false

- input_type: log
  encoding: GB2312
 # fields_under_root: true
  fields:
    #serverip: 192.168.1.10
    logtopic: dmesg
  enabled: True
  paths:
        - /var/log/dmesg
  multiline.pattern: '^\['
  multiline.negate:  true
  multiline.match: after
  tail_files: false

- input_type: log
  encoding: GB2312
 # fields_under_root: true
  fields:
    #serverip: 192.168.1.10
    logtopic: secure
  enabled: True
  paths:
        - /var/log/secure
  multiline.pattern: '^\['
  multiline.negate:  true
  multiline.match: after
  tail_files: false
#----------------------------- Logstash output --------------------------------
output.kafka:
  enabled: true
  hosts: ["192.168.7.223:9092", "192.168.7.224:9092", "192.168.7.227:9092"]
  topic: 'onecloud-%{[beat.hostname]}-%{[fields.logtopic]}-%{+yyyy.MM.dd}' ##匹配fileds字下的logtopic
  partition.hash:
    reachable_only: true
  compression: gzip
  max_message_bytes: 1000000
  required_acks: 1
logging.to_files: true
```

查看配置文件内容/etc/filebeat/filebeat.yml，直接写入ES

```
# cat filebeat.yml
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /var/log/messages
  fields:
    log_type: "messages"
- type: log
  enabled: true
  paths:
    - /var/log/dmesg
  fields:
    log_type: "dmesg"
  multiline.pattern: '^\s'
  multiline.negate: true
  multiline.match: after
- type: log
  enabled: true
  paths:
    - /var/log/secure
  fields:
    log_type: "secure"
  multiline.pattern: '^\s'
  multiline.negate: true
  multiline.match: after
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: true
setup.template.settings:
  index.number_of_shards: 3
setup.kibana:
  host: "192.168.7.228:5601"
output.elasticsearch:
  hosts: ["192.168.7.232:9200","192.168.7.231:9200","192.168.7.229:9200"]
  index: "onecloud-%{[beat.hostname]}-message-%{+yyyy.MM.dd}"
  indices:
    - index: "onecloud-%{[beat.hostname]}-dmesg-%{+yyyy.MM.dd}"
      when.contains:
        fields:
          log_type: "dmesg"
    - index: "onecloud-%{[beat.hostname]}-secure-%{+yyyy.MM.dd}"
      when.contains:
        fields:
          log_type: "secure"
setup.template.name: "onecloud"
setup.template.pattern: "onecloud-*"
setup.template.enabled: false
setup.template.overwrite: true
processors:
  - add_host_metadata: ~
  - add_cloud_metadata: ~
```

Done

原文链接：ELK 日志平台 logstash 和 filebeat