ELK（三）：nginx+filebeat+redis

作者：zengxiaoyun

原文链接：https://ld246.com/article/1503473347347

来源网站：链滴

1. 调整nginx的access日志格式为json

```
log_format json '{"@timestamp":"$time_iso8601",'
                '"source":"nginxgold56",'
                '"serverAddr":"$server_addr",'
                '"remoteAddr":"$remote_addr",'
                '"remoteUser":"$remote_user",'
                '"size":$body_bytes_sent,'
                '"status":$status,'
                '"time":$request_time,'
                '"method":"$request_method",'
                '"protocol":"$server_protocol",'
                '"url":"$scheme://$host$request_uri",'
                '"host":"$http_host",'
                '"uri":"$uri",'
                '"referer":"$http_referer",'
                '"xforwarded":"$http_x_forwarded_for",'
                '"agent":"$http_user_agent",'
                '"upsTime":"$upstream_response_time",'
                '"sslPro":"$ssl_protocol",'
                '"sslCip":"$ssl_cipher",'
                '"upsStatus":"$upstream_status"}';

access_log logs/access.log json;
```

2. filebeat读取nginx日志到redis

2.1. 安装filebeat

```
#下载fielbeat
cd /opt/install
wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-5.5.1-linux-x86_64.tar.gz

#解压
tar -zxvf filebeat-5.5.1-linux-x86_64.tar.gz -C /opt/app/

#重命名
cd /opt/app/
mv mv filebeat-5.5.1-linux-x86_64 filebeat
```

2.2. 配置filebeat

```
vim filebeat/filebeat.yml
```

2.2.1. 配置filebeat.prospectors读取nginx access日志

```
filebeat.prospectors:
- input_type: log
  paths:
    #nginx日志位置
```

```
    - /usr/local/nginx/logs/access.log
  #相当于elk的表名
  document_type: gold
  #ngxin的json日志作为根
  json.keys_under_root: true
  #覆盖filebeat自身的字段
  json.overwrite_keys: true
```

2.2.2. 配置output.redis输出到redis服务器

```
output.redis:
  enabled: true
  hosts: ["192.168.254.210:6379"]
  key: logstash
  datatype: list
```

2.2.3. 配置path

```
#filebeat安装目录
path.home: /usr/local/filebeat
#filebeat数据目录
path.data: /usr/local/filebeat/data
#filebeat日志目录
path.logs: /usr/local/filebeat/logs
```

2.2.4. 配置filebeat自身日志参数

```
logging.to_files: true
logging.files:
  #每个日志文件大小
  rotateeverybytes: 10485760
  #最多保存N个日志文件
  keepfiles: 10
```

3. 启动filebeat

```
nohup /opt/app/filebeat/filebeat >/dev/null 2>&1 &
```

附filebeat文件：filebeat.yml