日志收集1.0

1、概述

所有系统的日志将通过 ElasticSearch + Logstash + Kibana 来收集系统的日志方便查看系统异常问题。

2、配置Nginx 日志格式

Nginx配置

```
# nginx
# log_format
log_format  main  '{ "@timestamp": "$time_iso8601", '
            '"@server_addr":"$server_addr",'
            '"hostname": "$hostname", '
            '"client": "$remote_addr", '
            '"host": "$host", '
            '"method":"$request_method",'
            '"status": "$status", '
            '"request_time": "$request_time", '
            '"request": "$request", '
            '"sent": "$body_bytes_sent", '
            '"content_len": "$content_length", '
            '"fw_ip": "$http_x_forwarded_for", '
            '"up_addr": "$upstream_addr", '
            '"up_status": "$upstream_status", '
            '"up_conn_time": "$upstream_connect_time", '
            '"up_resp_time": "$upstream_response_time", '
            '"referer": "$http_referer", '
                       '"ua": "$http_user_agent" }';
# nginx
access_log /var/log/nginx/dmp.log main;
```

3、安装logstash

官网安装说明

4、配置logstash.conf

logstash配置

```
input {
    file {
        path => [ "/var/log/nginx/dmp.log" ]
        codec => json
        }
}

filter {
    mutate {
        convert => [ "status","integer" ]
        convert => [ "sent","integer" ]
        convert => [ "content_len","integer" ]
        convert => [ "request_time","float" ]
        convert => [ "up_conn_time","float" ]
        convert => [ "up_resp_time","float" ]
        split => ["fw_ip",","]
        add_field => ["real_remote_addr","%{fw_ip[0]}"]
 #        remove_field => "message"
    }

    geoip {
        source => "real_remote_addr"
        target => "geoip"
        fields => [ "location", "city_name", "country_name", "region_name"
]
    }
}


output {
    elasticsearch {
        hosts => ["ip1:9200","ip2:9200","ip3:9200"]
        index => "logstash-dmp-jingzhi-access-%{+YYYY.MM.dd}"
        template_overwrite => "true"
        manage_template => "true"
    }
}
```

5、启动测试:

/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/baijiuyun.com

(logstash 安装地址 -f 配置文件地址)

注意： 如有多个配置文件在同一台启动，可以使用 /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/* 来执行。

6、持久执行使用supervisord

supervisord :

ubuntu:

```
apt install supervisor
```

```
vim /etc/supervisor/supervisord.conf
```

supervisord通用配置

```
;supervisor config file

[unix_http_server]
file=/var/run/supervisor.sock   ; (the path to the socket file)
chmod=0770                       ; sockef file mode (default 0700)

[supervisord]
logfile=/var/log/supervisor/supervisord.log ; (main log file;default $CWD
/supervisord.log)
pidfile=/var/run/supervisord.pid ; (supervisord pidfile;default
supervisord.pid)
childlogdir=/var/log/supervisor            ; ('AUTO' child log dir,
default $TEMP)

; the below section must remain in the config file for RPC
; (supervisorctl/web interface) to work, additional interfaces may be
; added by defining them in separate rpcinterface: sections
[rpcinterface:supervisor]
supervisor.rpcinterface_factory = supervisor.rpcinterface:
make_main_rpcinterface

[supervisorctl]
serverurl=unix:///var/run/supervisor.sock ; use a unix:// URL  for a unix
socket

; The [include] section can just contain the "files" setting.  This
; setting can list multiple files (separated by whitespace or
; newlines).  It can also contain wildcards.  The filenames are
; interpreted as relative to this file.  Included files *cannot*
; include files themselves.

[include]
files = /etc/supervisor/conf.d/*.conf
```

增加supervisord配置文件

```
vim /etc/supervisor/conf.d/logstash.conf
```

supervisord 配置文件

```
[supervisord]
minfds=65536
minprocs=3276
[program:logstash]
autorestart=true  ;
;environment=JAVA_HOME=/opt/jdk1.8.0_151/ ;java
user=root
directory=/usr/share/logstash/bin/  ;
command=/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/* ;
stdout_logfile_maxbytes = 20MB ;
stdout_logfile_backups = 10 ;
stdout_logfile = /opt/logs/logstash.log ;
```

执行命令: supervisorctl update

supervisorctl status logstash 查看logstash 执行状态

查看9600端口是否执行，logstash 成果启动。

```
root@Test1:/var/log/nginx# lsof -i:9600
COMMAND   PID USER   FD   TYPE   DEVICE SIZE/OFF NODE NAME
java    23123 root   88u  IPv4 27008643      0t0  TCP localhost:9600
(LISTEN)
```