

小喵爱你

xiaomlove

PHP

WordPress

JS/JQ

HTML/CSS

Mysql

IOS

Skill

友链

其他

Website&Blog

Home » Code » 使用goaccess对Nginx日志简单分析

使用GOACCESS对NGINX日志简单分析

Posted by: xiaomiao 2019/04/01 in Code, Linux Leave a comment

接[上篇](#)使用 Linux命 令来分析。使用命令太麻烦，既不快捷又不直观，市面上有不少现成的工具可以使用，比如 ELK。但 ELK 太重了，这里使用的是比较轻量的 [goaccess](#)。

接收日志

goaccess 是直接对日志文件进行分析，首先要获得日志文件。nginx 原生支持将日志发送到远程 syslog，参见[官方文档](#)。

```
1 | access_log syslog:server=xxx.xxx.xxx.xxx:514,facility=local5,tag=access_lc
```

对于接收端，配置 rsyslog 接收数据。

```
1 # Provides UDP syslog reception
2 $ModLoad imudp
3 $UDPServerRun 514
4
5 # Provides TCP syslog reception
6 $ModLoad imtcp
7 $InputTCPServerRun 514
8
9 # 定义两个模板，一个生成动态文件，一个替换默认的日志格式
10 template (name="nginx_access_file" type="string" string="/opt/nginx-logs/
11 template (name="nginx_access_format" type="string"
12 string="%msg:2:$%\n")
13
14 # 接收 facility 为 local5 的日志
15 local5.* action(type="omfile" dynafilename="nginx_access_file" template="ngir
```

接收端口514，UDP 和 TCP 协议都开了。

关于模板，得参考 rsyslog 官方文档，其中 %programname% 其实跟 %syslogtag% 一样，只是后者多了个：，并不需要，所以使用 %programname%。全部可用属性参见[这里](#)。日志格式为何不直接使用 %msg% 呢，原因是它使用的某个标准开头就是有空格，我们并不需要，需要去掉，参见[此文](#)。

关于 action，type 是必须的，指定输出模块，type 或 dynafilename 必须其一，指定输出到静态文件或动态文件（动态优先），template 指定所用模板。

rsyslog 配置一大堆，写错又不报，可以通过这个命令来检查是否正确：rsyslogd -N1，参见[这里](#)。

分析日志

依据文档[安装 goaccess](#)：

```
1 $ wget https://tar.goaccess.io/goaccess-1.3.tar.gz
2 $ tar -xvzf goaccess-1.3.tar.gz
3 $ cd goaccess-1.3/
4 $ ./configure --enable-utf8 --enable-geoip=mmdb --enable-tcb=btrees
5 $ make
6 # make install
```

这里 --enable-geoip=mmdb，是使用 geoip 的城市数据库（通过 IP 获得城市），缺少什么搜索都能解决，注意别忘了 libmaxminddb-devel.x86_64。由于enable-tcb=btrees(开多个指定数据位置需要)，还需要yum install tokyocabinet-devel bzip2-devel zlib-devel。

在开始之前先要进行必要的配置，配置文件是：goaccess.conf，不知道在哪里全局搜索一下，比如我的位于：/usr/local/etc/goaccess/goaccess.conf。必须配置的字段是time_format、date_format、log_format，在[faq 页面](#)有说明有网友提供了一个工具 [nginx2goaccess](#)，输入日志格式是得出配置信息：

近期文章

- 经典sql难题——组内极值
- Laravel文件系统
- Linux使用mail发送邮件
- 使用goaccess对Nginx日志简单分析
- 使用Linux命令对Nginx日志进行简单统计

近期评论

- Check This发表在《torrent种子结构解析与B编码》
- kolb发表在《Laravel Nova安装》
- aidiie发表在《Laravel Nova安装》
- 灯火阑珊发表在《Laravel Nova安装》
- Anthonyjab发表在《php安装gearman扩展实现异步分步式任务》

文章归档

- 2019年五月 (1)
- 2019年四月 (3)
- 2019年三月 (4)
- 2018年十一月 (1)
- 2018年十月 (1)
- 2018年九月 (1)
- 2018年八月 (1)
- 2018年六月 (2)
- 2018年五月 (1)
- 2018年四月 (1)
- 2018年三月 (1)
- 2017年十月 (3)
- 2017年九月 (2)
- 2017年八月 (1)
- 2017年五月 (3)
- 2017年四月 (4)
- 2017年一月 (4)
- 2016年十二月 (2)
- 2016年十一月 (3)
- 2016年十月 (1)
- 2016年九月 (1)
- 2016年七月 (3)
- 2016年六月 (3)
- 2016年五月 (6)
- 2016年四月 (3)
- 2016年三月 (10)
- 2016年二月 (5)
- 2016年一月 (8)
- 2015年十二月 (2)
- 2015年十一月 (8)
- 2015年十月 (9)
- 2015年九月 (9)
- 2015年八月 (5)
- 2015年七月 (7)
- 2015年六月 (3)
- 2015年五月 (19)

```
1 [root@VM_0_9-centos ~]# ./nginx2goaccess.sh '$remote_addr - $remote_user [  
2  
3 - Generated goaccess config:  
4  
5 time-format %T  
6 date-format %d/%b/%Y  
7 log_format %h - %^ [%d:%t %^] "%r" %s %b "%R" "%u" "%^" %T %^
```

然后在配置文件末尾添加这三项即可。由于还要使用 geoip 数据库，最终添加了四项：

```
1 time-format %T  
2 date-format %d/%b/%Y  
3 log_format %h - %^ [%d:%t %^] "%r" %s %b "%R" "%u" "%^" %T %^  
4 geoip-database /usr/local/src/GeoLite2-City_20190326/GeoLite2-City.mmdb
```

最后，执行以下命令，即可生成报告：

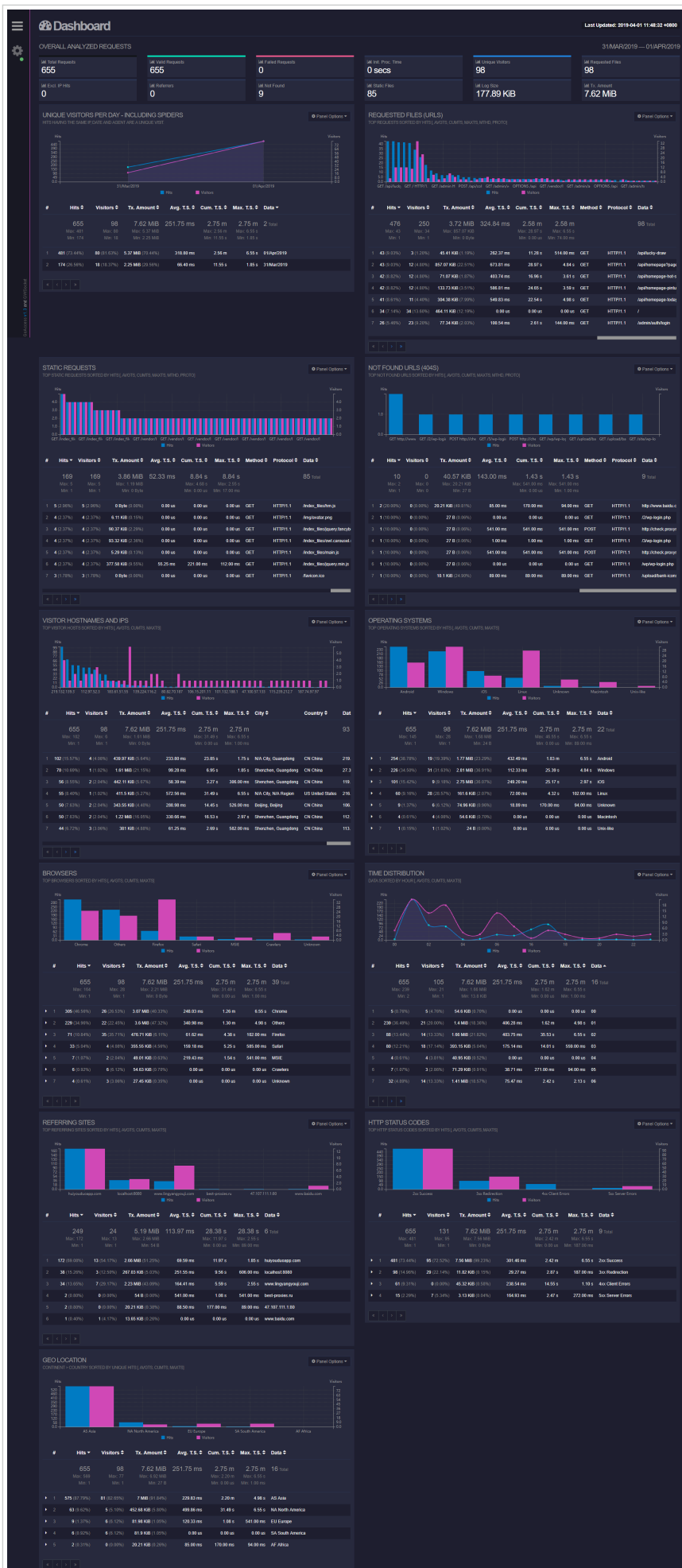
```
~/local/etc/goaccess/goaccess.conf -o report.html --real-time-html --daemonize
```

其中 -o 是生成的文件所在目录，放到一个可通过 web 访问下目录即可。最终结果：

2015年四月 (20)
2015年三月 (3)
2015年二月 (3)
2015年一月 (11)
2014年十二月 (9)
2014年十一月 (8)
2014年十月 (7)
2014年九月 (4)
2014年八月 (2)
2014年七月 (3)
2014年六月 (8)
2014年五月 (11)

分类目录

Code (213)
C# (1)
HTML/CSS (22)
IOS (19)
Object-c (7)
Swift (11)
JS/JQ (72)
Linux (20)
Mysql (14)
PHP (85)
Laravel (10)
WordPress (15)
Movie (2)
Skill (7)
未分类 (9)



PS, 如果有多个网站, 就起多个 goaccess 进程, 直接写完整的命令即可 (注意使用不同的 socket 端口、fifo-in、fifo-out、pid-file):

```
1 goaccess /opt/nginx-logs/access_log_huanbao.log \  
2 -o /usr/share/nginx/html/laravel/public/huanbao.html \  
3 --time-format '%T' \  
4 --date-format '%d/%b/%Y' \  
5 --log-format '%h - %^ [%d:%t %^] "%r" %s %b "%R" "%u" "%^" %T %^ "%^"' \  
6 --geoip-database /usr/local/src/GeoLite2-City_20190326/GeoLite2-City.mmdb \  
7 --db-path /tmp/goaccess/huanbao \  
8 --fifo-in /tmp/goaccess/huanbao/fifo.in \  
9 --fifo-out /tmp/goaccess/huanbao/fifo.out \  
10 --pid-file /tmp/goaccess/huanbao/goaccess.pid \  
11 --real-time-html \  
12 --port 7891 \  
13 --daemonize
```

参见[这里](#)。

<<

Previous:
使用Linux命令对Nginx日志进行简单统计

Next:
Linux使用mail发送邮件

>>

RELATED ARTICLES

经典sql难题——组内极值	Laravel文件系统	Linux使用mail发送邮件
2019/05/26	2019/04/21	2019/04/06

LEAVE A REPLY


Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Time limit is exhausted. Please reload CAPTCHA.

八 × 5 = 

Post Comment

