# Apache开启详细访问日志

|  |  |
| --- | --- |
| 文档编辑人 | 岳现伦 |
| 日期 | 2017-11-23 |
| 版本 | V1 |

## 目的

本文档将apache日志的详细信息进行记录包括cookie信息，refer信息等等，监控该详细详细并将该信息提供给告警接入平台进行分析。

## 1 加载mod\_usertrack模块

默认情况下该模块没有加载

### 检查该模块是否安装

|  |
| --- |
| ***root@mid-1 bin]# ./apachectl -M***  httpd: Could not reliably determine the server''s fully qualified domain name, using 192.168.56.60 for ServerName  Loaded Modules:  core\_module (static)  authn\_file\_module (static)  authn\_default\_module (static)  authz\_host\_module (static)  authz\_groupfile\_module (static)  authz\_user\_module (static)  authz\_default\_module (static)  auth\_basic\_module (static)  include\_module (static)  filter\_module (static)  log\_config\_module (static)  env\_module (static)  setenvif\_module (static)  version\_module (static)  mpm\_prefork\_module (static)  http\_module (static)  mime\_module (static)  status\_module (static)  autoindex\_module (static)  asis\_module (static)  cgi\_module (static)  negotiation\_module (static)  dir\_module (static)  actions\_module (static)  userdir\_module (static)  alias\_module (static)  so\_module (static)  Syntax OK  ***[root@mid-1 bin]# ./apachectl -M |grep user***  httpd: Could not reliably determine the server''s fully qualified domain name, using 192.168.56.60 for ServerName  Syntax OK  authz\_user\_module (static)  userdir\_module (static)  ----检查未发现该模块 则需要加载该模块 |

### 1.2加载mod\_usertrack模块

|  |
| --- |
| ***---模块在http的原始安装包上存在，通过下面的方式进行查找原始的c文件***  ***[root@mid-1 httpd-2.2.34]# find ./ -name mod\_usertrack\****  ./modules/metadata/mod\_usertrack.exp  **./modules/metadata/mod\_usertrack.c**  ./modules/metadata/mod\_usertrack.mak  ./modules/metadata/mod\_usertrack.dep  ./modules/metadata/mod\_usertrack.dsp  ./docs/manual/mod/mod\_usertrack.html  ./docs/manual/mod/mod\_usertrack.html.en  ***[root@mid-1 metadata]# cd ./modules/metadata/***  [root@mid-1 metadata]# ls mod\_usertrack.c  mod\_usertrack.c  ***找到该文件 将这个扩展到当前的apache上去***  ***[root@mid-1 metadata]# /apache/apache2\_2/bin/apxs -i -a -c mod\_usertrack.c***  /usr/lib64/apr-1/build/libtool --silent --mode=compile gcc -prefer-pic -DLINUX=2 -D\_REENTRANT -D\_GNU\_SOURCE -pthread -I/apache/apache2\_2/include -I/usr/include/apr-1 -I/usr/include/apr-1 -c -o mod\_usertrack.lo mod\_usertrack.c && touch mod\_usertrack.slo  /usr/lib64/apr-1/build/libtool --silent --mode=link gcc -o mod\_usertrack.la -rpath /apache/apache2\_2/modules -module -avoid-version mod\_usertrack.lo  /apache/apache2\_2/build/instdso.sh SH\_LIBTOOL='/usr/lib64/apr-1/build/libtool' mod\_usertrack.la /apache/apache2\_2/modules  /usr/lib64/apr-1/build/libtool --mode=install cp mod\_usertrack.la /apache/apache2\_2/modules/  cp .libs/mod\_usertrack.so /apache/apache2\_2/modules/mod\_usertrack.so  cp .libs/mod\_usertrack.lai /apache/apache2\_2/modules/mod\_usertrack.la  cp .libs/mod\_usertrack.a /apache/apache2\_2/modules/mod\_usertrack.a  chmod 644 /apache/apache2\_2/modules/mod\_usertrack.a  ranlib /apache/apache2\_2/modules/mod\_usertrack.a  PATH="$PATH:/sbin" ldconfig -n /apache/apache2\_2/modules  ----------------------------------------------------------------------  Libraries have been installed in:  /apache/apache2\_2/modules  If you ever happen to want to link against installed libraries  in a given directory, LIBDIR, you must either use libtool, and  specify the full pathname of the library, or use the `-LLIBDIR'  flag during linking and do at least one of the following:  - add LIBDIR to the `LD\_LIBRARY\_PATH' environment variable  during execution  - add LIBDIR to the `LD\_RUN\_PATH' environment variable  during linking  - use the `-Wl,--rpath -Wl,LIBDIR' linker flag  - have your system administrator add LIBDIR to `/etc/ld.so.conf'  See any operating system documentation about shared libraries for  more information, such as the ld(1) and ld.so(8) manual pages.  ----------------------------------------------------------------------  chmod 755 /apache/apache2\_2/modules/mod\_usertrack.so  [activating module `usertrack' in /apache/apache2\_2/conf/httpd.conf]  ***-----扩展完成***  ***检查模块是否已经存在***  [root@mid-1 apache2\_2]# ls  bin build cgi-bin conf error htdocs icons include logs man manual modules  ***[root@mid-1 apache2\_2]# cd modules/***  [root@mid-1 modules]# ls  httpd.exp mod\_usertrack.so  [root@mid-1 modules]# cd ..  ***[root@mid-1 apache2\_2]# cd bin***  ***[root@mid-1 bin]# ./apachectl -M***  httpd: Could not reliably determine the server's fully qualified domain name, using 192.168.56.60 for ServerName  Loaded Modules:  core\_module (static)  authn\_file\_module (static)  authn\_default\_module (static)  authz\_host\_module (static)  authz\_groupfile\_module (static)  authz\_user\_module (static)  authz\_default\_module (static)  auth\_basic\_module (static)  include\_module (static)  filter\_module (static)  log\_config\_module (static)  env\_module (static)  setenvif\_module (static)  version\_module (static)  mpm\_prefork\_module (static)  http\_module (static)  mime\_module (static)  status\_module (static)  autoindex\_module (static)  asis\_module (static)  cgi\_module (static)  negotiation\_module (static)  dir\_module (static)  actions\_module (static)  userdir\_module (static)  alias\_module (static)  so\_module (static)  **usertrack\_module (shared)**  Syntax OK  ----已加载  同时加载下面的模块  LoadModule logio\_module modules/mod\_logio.so  该so 的作用就是记录日志大小的中的input 和output 的大小， 按照上面的方式将该module加载上去  在下文当中的的%I %O必须使用该模块。 |

## 2配置apache 的httpd.conf文件

### 2.1配置cookie记录

|  |
| --- |
| --  ***[root@mid-1 conf]# pwd***  ***/apache/apache2\_2/conf***  ***[root@mid-1 conf]# vi httpd.conf***  # Example:  # LoadModule foo\_module modules/mod\_foo.so  在下面添加如下信息  ***LoadModule usertrack\_module modules/mod\_usertrack.so***  ***<IfModule usertrack\_module>***  ***CookieStyle RFC2965***  ***CookieTracking on***  ***</IfModule>***  修改LogFormat日志信息  <IfModule log\_config\_module>  #  # The following directives define some format nicknames for use with  # a CustomLog directive (see below).  #  LogFormat "%h %l D=%D %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""combined  LogFormat "%h %l %u %t \"%r\" %>s %b" common ***<<<<<<<<修改该行信息添加cookie日志格式***  ····················································  # logged therein and \*not\* in this file.  #  ***CustomLog "logs/access\_log" common***  因目前日志记录使用的该common模式因此修改common模式下的日志格式。  ---当然也可以定制其他样式的格式需要添加新一行的logFormat和修改Customlog 日志  ---例如  --- 添加行 LogFormat "%h %l D=%D %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""cookie\_log  -----添加行 CustomLog "logs/cookie\_log " cookie\_log  修改后如下  ***LogFormat "%h %l %u %t \"%r\" %>s %b \"%{COOKIE}n\" " common*** |

### 2.2 开启其他apache日志信息

|  |
| --- |
| ***[root@mid-1 conf]# pwd***  ***/apache/apache2\_2/conf***  ***[root@mid-1 conf]# vi httpd.conf***  LogFormat "%h %l D=%D %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""combined  LogFormat "%h %l %u %t \"%r\" %>s %b" common ***<<<<<<<<修改该行信息添加cookie日志格式***  ····················································  # logged therein and \*not\* in this file.  #  ***CustomLog "logs/access\_log" common***  因目前日志记录使用的该common模式因此修改common模式下的日志格式。  修改后如下所示  ***LogFormat "s=%s s2=%>s x=%X t=%t a=%a h=%h A=%A B=%B b=%b D=%D T=%T f=%f m=%m h=%h p=%p H=%H P=%P r=\"%r\" l=%l format\_P=\"%{format}P\" q=%q u=%u U=%U v=%v V=%V foobar\_c=\"%{Foobar}C\" foobar\_i=\"%{Foobar}i\" foobar\_n=\"%{Foobar}n\" foobar\_o=\"%{Foobar}o\" referer\_i=\"%{Referer}i\" user\_agent\_i=\"%{User-Agent}i\" cookie\_n=\"%{COOKIE}n\" I=%I O=%O Foobar\_e=\"%{FOOBAR}e\"" common*** |

### 2.3 开启后收集的信息示例

|  |
| --- |
| 日志示例：  ***[root@mid-1 logs]# pwd***  ***/apache/apache2\_2/logs***  ***[root@mid-1 logs]# tail -300f access\_log***  s=404 s2=404 x=+ t=[23/Nov/2017:17:00:46 +0800] a=192.168.56.102 h=192.168.56.102 A=192.168.56.60 B=209 b=209 D=509 T=0 f=/apache/apache2\_2/htdocs/favicon.ico m=GET h=192.168.56.102 p=80 H=HTTP/1.1 P=31909 r="GET /favicon.ico HTTP/1.1" l=- format\_P="format" q= u=- U=/favicon.ico v=192.168.56.60 V=192.168.56.60 foobar\_c="-" foobar\_i="-" foobar\_n="-" foobar\_o="-" referer\_i="http://192.168.56.60/" user\_agent\_i="Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" cookie\_n="192.168.56.102.1511427646343194" I=343 O=424 Foobar\_e="-"  s=200 s2=200 x=+ t=[23/Nov/2017:17:00:50 +0800] a=192.168.56.102 h=192.168.56.102 A=192.168.56.60 B=1088 b=1088 D=425 T=0 f=/apache/apache2\_2/htdocs/awr/ m=GET h=192.168.56.102 p=80 H=HTTP/1.1 P=31909 r="GET /awr/ HTTP/1.1" l=- format\_P="format" q= u=- U=/awr/ v=192.168.56.60 V=192.168.56.60 foobar\_c="-" foobar\_i="-" foobar\_n="-" foobar\_o="-" referer\_i="http://192.168.56.60/" user\_agent\_i="Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" cookie\_n="192.168.56.102.1511427650864821" I=412 O=1355 Foobar\_e="-"cookie\_n="192.168.56.102.1511423264027124" I=494 O=979855 Foobar\_e="-" |

### 2.4 各种格式所代表的日志级别

|  |
| --- |
| %% 百分号(Apache2.0.44或更高的版本)  %a 远端IP地址  %A 本机IP地址  %B 除HTTP头以外传送的字节数  %b 以CLF格式显示的除HTTP头以外传送的字节数，也就是当没有字节传送时显示'-'而不是0。  %{Foobar}C 在请求中传送给服务端的cookieFoobar的内容。  %D 服务器处理本请求所用时间，以微为单位。  %{FOOBAR}e 环境变量FOOBAR的值  %f 文件名  %h 远端主机  %H 请求使用的协议  %{Foobar}i 发送到服务器的请求头Foobar:的内容。  %l 远端登录名(由identd而来，如果支持的话)，除非IdentityCheck设为"On"，否则将得到一个"-"。  %m 请求的方法  %{Foobar}n 来自另一个模块的注解Foobar的内容。  %{Foobar}o 应答头Foobar:的内容。  %p 服务器服务于该请求的标准端口。  %P 为本请求提供服务的子进程的PID。  %{format}P 服务于该请求的PID或TID(线程ID)，format的取值范围为：pid和tid(2.0.46及以后版本)以及hextid(需要APR1.2.0及以上版本)  %q 查询字符串(若存在则由一个"?"引导，否则返回空串)  %r 请求的第一行  %s 状态。对于内部重定向的请求，这个状态指的是原始请求的状态，--%>s则指的是最后请求的状态。  %t 时间，用普通日志时间格式(标准英语格式)  %{format}t 时间，用strftime(3)指定的格式表示的时间。(默认情况下按本地化格式)  %T 处理完请求所花时间，以秒为单位。  %u 远程用户名(根据验证信息而来；如果返回status(%s)为401，可能是假的)  %U 请求的URL路径，不包含查询字符串。  %v 对该请求提供服务的标准ServerName。  %V 根据UseCanonicalName指令设定的服务器名称。  %X 请求完成时的连接状态：  X= 连接在应答完成前中断。  += 应答传送完后继续保持连接。  -= 应答传送完后关闭连接。  (在1.3以后的版本中，这个指令是%c，但这样就和过去的SSL语法：%{var}c冲突了)  %I 接收的字节数，包括请求头的数据，并且不能为零。要使用这个指令你必须启用mod\_logio模块。  %O 发送的字节数，包括请求头的数据，并且不能为零。要使用这个指令你必须启用mod\_logio模块。  %s 返回的结果解析  HTTP状态码  1xx：信息性状态码  100 请求继续  2xx：成功状态码  200：OK  201：Created  3xx：重定向的状态码  301：Moved Permanently 永久重定向 在响应报文中使用"Location：URL"指定资源现在所处的位置  302：Found 临时重定向 在响应报文中使用首部"Location：URL" 指定临时资源位置  304：Not Modified，条件或请求中使用  4xx：客户端类的错误  403：Forbidden，请求被服务器拒绝  404：Not Found 服务器无法找到请求的URL  405：Method Not Allowed,不允许使用此方法请求相应的URL  5xx：服务器端的错误  500：Internal Server Error，服务器内部错误（比如权限错误）  502：Bad Gateway 代理服务器从上游收到的一条伪响应  503：Service Unavaliable，服务器此时无法提供服务，但将来可能可用 |

***-------the end***